Innovation-Based Remote State Estimation Secrecy with no Acknowledgments

Justin M. Kennedy *Member, IEEE*, Jason J. Ford,
Daniel E. Quevedo *Fellow, IEEE* and Falko Dressler *Fellow, IEEE*

***Abstract*—Secrecy encoding for remote state estimation in the presence of adversarial eavesdroppers is a well studied problem. Typical existing secrecy encoding schemes rely on the transmitter's knowledge of the remote estimator's current performance. This performance measure is often shared via packet receipt acknowledgments. However, in practical situations the acknowledgment channel may be susceptible to interference from an active adversary, resulting in the secrecy encoding scheme failing. Aiming to achieve a reliable state estimate for a legitimate estimator while ensuring secrecy, we propose a secrecy encoding scheme without the need for packet receipt acknowledgments. Our encoding scheme uses a pre-arranged scheduling sequence established at the transmitter and legitimate receiver. We transmit a packet containing either the state measurement or encoded information for the legitimate user. The encoding makes the packet appear to be the state but is designed to damage an eavesdropper's estimate. The pre-arranged scheduling sequence and encoding is chosen psuedo-random. We analyze the performance of our encoding scheme against a class of eavesdropper, and show conditions to force the eavesdropper to have an unbounded estimation performance. Further, we provide a numerical illustration and apply our encoding scheme to an application in power systems.**

***Index Terms*—Remote State Estimation, Eavesdropping, Privacy, State-Secrecy Codes**

I. INTRODUCTION

THE emerging network of cyber-physical systems has been acknowledged as a vulnerability [1] with recent incidents drawing attention to the need to improve the security of these systems [2]. Ensuring security of cyber-physical systems can be enhanced through control-theoretic approaches including through the utilization of the dynamics in the design [3]. Three key security problems exist: ensuring confidentiality of state information and control actions, integrity of transmissions, and availability of data over a network [4]. In this article we focus on the problem of confidential state estimation of a remote process over an unreliable wireless channel in the presence of an eavesdropper.

While the interest in control systems design is the closed-loop system performance, it is first necessary to ensure the quality of the state estimate used in the controller. Sharing state information at every time instant provides valuable information to a legitimate user. However, as transmissions can be intercepted by an adversarial eavesdropper, which could use transmitted state information to design future attacks on the system [5], it becomes necessary to obfuscate the shared state estimate from an eavesdropper. This motivates private remote state estimation techniques to ensure state secrecy. Recent works have shown that through careful scheduling of transmissions [6]–[8] or by encrypting the packets [9]–[12], significant reduction in adversary performance can be achieved at the cost of modest degradation in legitimate user performance. We shall explore this trade-off in our design.

Many state secrecy techniques require knowledge of the legitimate estimator's current performance, often shared through acknowledgment of successful packet receipt. Scheduling the next transmission from the legitimate user's last received packet can be used to create the illusion of a random transmission policy to an eavesdropper [7]. By relying heavily on acknowledgments, [11] showed that an encoded transmission of relative measurement, the innovation between the current state and the last acknowledged packet, diverges an eavesdropper's estimate. In the case of a *critical event* where the eavesdropper misses a packet that the legitimate receiver obtains, the eavesdropper is unable to recover the state estimate, and its estimation error will constantly grow.[1] Effectively, the use of innovations with acknowledgments, can provide so-called infinite secrecy of the state information.

However, in many practical situations an acknowledgment channel may be unavailable due to hardware limitations, such as for small power limited sensors [13], [14], or an adversary jamming the network [15]. Under the encoding scheme of [11], for an eavesdropper to maintain knowledge of the state, the adversary needs to prevent the critical event from occurring. An active eavesdropper that combines both eavesdropping and acknowledgment blocking tasks simultaneously, such as considered in [15], could block all acknowledgments or be stealthy and only block acknowledgments when the critical event occurs thus hiding in the stochastic nature of the net-

This work has been supported in part by the project NICCI2 funded by the German Research Foundation (DFG) under grant numbers DR 639/23-2 and QU 437/1-2.

JK, JF, and DQ acknowledge continued support from the Queensland University of Technology (QUT) through the Centre for Robotics.

J. M. Kennedy, J. J. Ford, and D. E. Quevedo are with the School of Electrical Engineering and Robotics, Queensland University of Technology, 2 George St, Brisbane QLD, 4000 Australia. F. Dressler is with the School of Electrical Engineering and Computer Science, TU Berlin, Germany. {j12.kennedy, j2.ford, daniel.quevedo}@qut.edu.au, dressler@ccs-labs.org

[1] The eavesdropper's estimation error will grow to infinity in the case of unstable dynamics [11] or to the open loop estimation error in the case of stable dynamics [10].

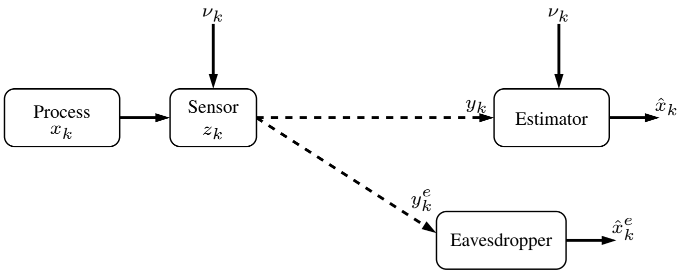

Fig. 1. Architecture of channel environment. A remote process sends state information over an unreliable wireless channel that can be received by the legitimate estimator and eavesdropper. The packet $\boldsymbol{z_k}$ is encoded with scheduling sequence $\boldsymbol{\nu_k}$ which is known exactly to the legitimate estimator but not the eavesdropper. The encoding does not rely on packet receipt acknowledgments.

work. This style of selective acknowledgment jamming attack has been demonstrated in practice on a carrier sense multiple access/collision avoidance (CSMA/CA) protocol WiFi network [16]. While it may be possible to detect a stealthy eavesdropper using statistical methods [17], the innovation state secrecy encoding scheme of [11] is no longer secret to this powerful eavesdropper.

As further background to our current work, we note that to improve an eavesdropper's performance, an adversary could exploit the vulnerability in packet acknowledgments, including through fake acknowledgment transmission [8] and event-based acknowledgment attacks [18]. Noting that often significant energy is required to block a communication channel, [19] proposed a strategy to balance performance degradation of the legitimate estimator with limited energy usage of the adversary. An active attack to damage the legitimate user's estimate is to transmit packets that appear, in a statistical sense, to be the state measurement [20], [21] alongside malicious control actions [22]. This has motivated watermarking schemes [23] and online statistical analysis [24] to ensure integrity of packets. In particular, to combat the denial of service attacks in large scale power networks, [25] proposed a distributed Kalman filter for state estimation, while [26] used the structured nature of the system to design a cooperative control approach.

In the present work, we are motivated to consider the problem of private remote state estimation without requiring receipt acknowledgments. The network architecture is visualized in Figure 1. We consider that the goal of the eavesdropper is to form a valid state estimate. While we consider that an adversarial eavesdropper could jam packets in the style of [16], this would deny the packet to all network users. As the eavesdropper wishes to form a valid state estimate, any adversarial attack is limited to acknowledgment channel blocking only. To damage an eavesdropper we propose an encoding scheme, where we randomly transmit either the state measurement or a random value that has the same statistical properties as the state. Inside the packet, we encode state information in the form of a single step innovation to improve performance of the legitimate user. The random encoding sequence is pre-arranged between the transmitter and legitimate user. Our proposal ensures the legitimate estimator has bounded performance and the system state remains secret to an eavesdropper. By increasing the proportion of encoded packets to unencoded packets, the secrecy against an eavesdropper is increased at the cost of legitimate estimator performance. We present our proposed encoding scheme in the sense of this trade-off.

Our work is inspired by the no acknowledgment secrecy scheme of [6], the use of some encrypted packets in [12], the innovation only encoding of [11], and the design of packets that force estimator divergence [20], [21]. To be more specific, we extend upon the design in [6] by sharing encoded information instead of no information thus improving the legitimate estimator performance without compromising security. Following the innovation encoding in [11], our encoded information is the single-step innovation which provides limited information to an eavesdropper with an already poor state estimate. However, as our transmission design is pre-arranged, the encoding is not subject to acknowledgment interference by an adversary. Inspired by [20], [21] we encode the packet with random noise that hides the usefulness of the packet and thereby increases divergence of the state estimation error covariance of a receiver. The key feature of our approach is that an uninformed eavesdropper may mistake the encoded packet as a state estimate. The design of the encoding is such that when inadvertently utilized as a state estimate by an eavesdropper, the estimation error covariance diverges providing a strong measure of secrecy.

Summary of contributions: We consider the problem of remote state estimation in the presence of eavesdroppers, and derive an encoding scheme to ensure secrecy of the state.

1) In contrast to many recent secrecy encoding schemes, such as [11] and [12], we consider the network environment of no packet receipt acknowledgments.
2) We improve on [6], by transmitting encoded state information that also damages the eavesdropper.
3) We derive expressions for the expected estimation error covariances as a function of the dynamics, channel quality, and encoding scheme.
4) We propose an offline designed scheduling sequence to achieve a suitable measure of state secrecy.

The remainder of the paper is structured as follows: we present the remote estimation scenario and pose our problem in Section II. In Section III we propose our encoding scheme and in Section IV give the performance for the legitimate estimator. In Section V we analyze the impact of our encoding scheme on a class of eavesdropper, and in Section VI provide guidance on scheduling design and numerical results. We illustrate application of our technique to a remote state estimation problem on a microgrid power system in Section VII. Finally, we provide concluding remarks in Section VIII.

Notation: At discrete time instances $k \geq 0$, x_k denotes the state of a process with dynamics A driven by zero-mean Gaussian process noise w_k with covariance Q from an initial state x_0 which is zero-mean distributed with covariance Σ_0. A sensor located at the process transmits a packet z_k containing either the state or encoded state information with noise χ_k, according to the pre-arranged sequence ν_k chosen pseudo-randomly with probability μ_d. The packet is received at the legitimate estimator (eavesdropper), indicated by γ_k (γ_k^e), with probability of success given by μ (μ_e). The legitimate estimator (eavesdropper) forms a state estimate $\hat{x}_{k|k}$ ($\hat{x}^e_{k|k}$) with estimation error covariance $P_{k|k}$ ($P^e_{k|k}$).

II. Remote State Estimation With an Eavesdropper

In this section we outline the dynamics and network model that we consider, and define the estimation of the legitimate estimator and eavesdropper.

A. System Dynamics

Consider a discrete-time LTI process with state $x_k \in \mathbb{R}^n$

$$x_{k+1} = Ax_k + w_k, \tag{1}$$

where w_k is a zero mean Gaussian distributed process with covariance Q, and A is marginally stable or unstable with at least one eigenvalue on or outside of the unit circle, respectively. Remote state estimation of unstable processes in the presence of eavesdroppers is an active problem, see for example [11], [24], [27], [28]. Additionally, many physical processes such as vehicle position or power systems [29] can be described with integrator models and are then marginally stable processes. For some cyber-physical processes the control unit and actuators may be separate from the sensors [28], [30], which under failure could result in open-loop operation, motivating estimation of marginally stable and unstable process.

We assume that the pair $(A, \sqrt{Q})$ is controllable, the initial state of the process x_0 is a Gaussian random variable with zero mean and covariance Σ_0, and that the two covariances Q and Σ_0 are positive definite. Additionally, we consider that w_k and x_0 are uncorrelated, and w_k and w_ℓ for $k \neq \ell$ are uncorrelated. Finally, we assume that properties of the process A, Q, and Σ_0 are public but the realization of the state x_0 and noise w_k are not known.

Remark 2.1: To achieve an optimal remote state estimate in the scenario that a sensor only has access to noisy measurements of the process, it has been suggested that a local filter should be operated at the sensor [31]. For a converged Kalman filter at the sensor, the dynamics of the sensor's local state estimate can be described by the pair (A, Q) where the process noise w_k represents the Kalman innovation. Thus the sensor's local state estimate has the same class of dynamics in (1) and the current method can be directly applied to such cases. See for example [11].

B. Channel Model

Following the standard packet based transmission utilized in network control problems, we consider that the sensor transmits a packet of state information, $z_k \in \mathbb{R}^p$, over an unreliable wireless channel to the legitimate estimator. The packets transmitted over the wireless channel can also be received by an eavesdropper with a separate antenna. To ensure privacy and secrecy of the state information, the packet is encoded. We propose our encoding scheme in Section III-B.

We consider a particularly challenging network situation where the packet receipts by the legitimate estimator are not acknowledged to the transmitting sensor. The lack of acknowledgment channel could be due to cost and energy usage [13], [14], or due to a powerful eavesdropper interfering [15], which has been demonstrated in practice for WiFi networks [16]. An encoding scheme that relies exclusively on acknowledgments, such as [11], may be rendered ineffective by acknowledgment blocking. While it is possible to detect such a powerful eavesdropper [17], an alternative technique that does not rely on acknowledgments to ensure privacy should be employed.

As there are no acknowledgments, the sensor does not have knowledge of the estimation performance of the legitimate estimator. Active privacy techniques which rely on knowledge of the remote estimator, such as scheduling [7] or encoding [11], are unsuitable here. Our proposed encoding scheme utilizes a pre-arranged scheduling sequence ν_k and encoding noise χ_k, known to the transmitting sensor and the legitimate estimator but is unknown to the eavesdropper. The encoding information is shared to the legitimate transmitter and estimator at system initialization, isolated from an adversary. Information security schemes commonly use pre-arranged security information in transmission encoding [32], cryptographic encryption [33], [34], and watermarking [20], [35]. The challenge in our work, is the design of encoding mechanism of the state information and the design of the scheduling sequence. Our network architecture is visualized in Figure 1.

Let us define $\gamma_k \in \{0, 1\}$ as an indicator variable denoting successful packet reception at the legitimate estimator where

$$\gamma_k = \begin{cases} 1, & \text{if the packet is received,} \\ 0, & \text{if a packet dropout occurs,} \end{cases} \tag{2}$$

and similarly $\gamma^e_k \in \{0, 1\}$ for outcomes at the eavesdropper. We assume that the channel outcomes for the estimator and eavesdropper are independent and identically distributed (i.i.d.), and that the channel outcomes are independent to the initial state of the process and the process noise. In a wireless communication environment, the channel characteristics for each user are assumed to be independent due to physically disjoint antenna [36]. This is due to the dependency of the signal distribution on the physical characteristics of the exact path between two antennas including all possible multi-path components due to reflections of the wireless signal. We define the channel qualities as the probability of successful packet receipt. We model these as Bernoulli random variables where, for the legitimate estimator, $\mathbb{P}(\gamma_k = 1) = \mu$ and, for the eavesdropper, $\mathbb{P}(\gamma^e_k = 1) = \mu_e$, where $0 \leq \mu, \mu_e \leq 1$. The channel qualities μ and μ_e are, thus, the complement of the probability of packet drop, i.e. $\mathbb{P}(\gamma_k = 0) = 1 - \mu$ and $\mathbb{P}(\gamma^e_k = 0) = 1 - \mu_e$. This model follows from standard wireless communication channels with block-fading over the channel links [37].

C. Minimum Mean Square Error Estimation

The estimates of the legitimate estimator and the eavesdropper depend on information available at each time in the received packets and knowledge of the scheduling sequence ν_k. Let us define the measurements as $y_k = \gamma_k z_k$, at the legitimate estimator, and $y^e_k = \gamma^e_k z_k$, at the eavesdropper. We define information available to the legitimate estimator at time k as $\mathcal{I}_k = \{\gamma_0, y_0, \nu_0, \gamma_1, y_1, \nu_1, \chi_1, \ldots, \gamma_k, y_k, \nu_k, \chi_k\}$ and $\mathcal{I}^e_k = \{\gamma^e_0, y^e_0, \ldots, \gamma^e_k, y^e_k\}$ for the eavesdropper. The legitimate estimator has perfect knowledge of the scheduling sequence ν_k and encoding noise χ_k, while the eavesdropper has no knowledge. The legitimate estimator's minimum mean square error (MMSE) estimate and associated covariance are defined as $\hat{x}_{k|k} = E[x_k|\mathcal{I}_k]$, $P_{k|k} = E[(x_k - \hat{x}_{k|k})(x_k - \hat{x}_{k|k})^\mathsf{T}|\mathcal{I}_k]$, and for the eavesdropper $\hat{x}^e_{k|k} = E[x_k|\mathcal{I}^e_k]$, $P^e_{k|k} = E[(x_k - \hat{x}^e_{k|k})(x_k - \hat{x}^e_{k|k})^\mathsf{T}|\mathcal{I}^e_k]$. We utilize the MMSE as a natural measure of state estimation performance as has been utilized in several privacy designs [7], [11], [18].

III. RANDOMIZED INNOVATION BASED ENCODING

In this section, we pose the secrecy requirements, propose our encoding scheme, and decoder for the legitimate estimator. In the following sections, we show the expected legitimate estimator performance, and provide guidance on encoding design choice for state secrecy against a class of eavesdropper.

A. State Secrecy

Our objective is to design an encoding scheme that produces a reliable state estimate at the legitimate estimator using no information of the current performance, while simultaneously ensuring poor estimation performance of an eavesdropper in the network. We introduce two notions of secrecy using the expectation of the MMSE of the legitimate estimator and the eavesdropper. A small MMSE indicates low estimation error and good state estimation performance, while a large MMSE indicates high estimation error and poor state estimation performance.

As our encoding scheme is designed with no information of the legitimate estimator's current estimate, we do not aim for optimal estimation at every packet receipt. Instead, we aim to ensure that the legitimate estimator's expected performance is upper bounded. To ensure secrecy of the state estimate we seek to design the encoding scheme such that an eavesdropper's expected MMSE is larger than the legitimate estimator's MMSE.

Definition 1 (Relative Secrecy): An encoding scheme achieves relative secrecy if and only if both the following conditions hold.

(i) There exists an $\Omega > 0$ such that the trace of the legitimate estimator's MMSE performance is upper bounded trace $E[P_{k|k}] < \Omega$ for all time $k > 0$.

(ii) The trace of the MMSE of the eavesdropper is strictly larger than that of the legitimate estimator trace $E[P_{k|k}] <$ trace $E[P^e_{k|k}]$ for all time $k > 0$.

We recall the definition of perfect secrecy from [6] to ensure that the eavesdropper's expected estimation error diverges to infinity, while the legitimate estimator's performance remains upper bounded.

Definition 2 (Perfect Secrecy): An encoding scheme achieves perfect secrecy if and only if both of the following conditions hold.

(i) There exists an $\Omega > 0$ such that the trace of the legitimate estimator's MMSE performance is upper bounded trace $E[P_{k|k}] < \Omega$ for all time $k > 0$.

(ii) The eavesdropper's expected MMSE is unbounded, or equivalently the trace diverges to infinity trace $E[P^e_{k|k}] \to \infty$ as $k \to \infty$.

For a remote state estimator of an unstable system always transmitting the state estimate over an unreliable wireless channel, i.e. $z_k = x_k$ for all $k > 0$, [38] showed that to ensure a bounded estimation error covariance, the network channel needs to satisfy

$$1 - \mu < \frac{1}{\rho(A)^2}, \text{ and } 1 - \mu_e < \frac{1}{\rho(A)^2}, \tag{3}$$

where $\rho(\cdot)$ is the spectral radius[2]. In this work, we assume that the channel qualities of both the legitimate estimator and eavesdropper satisfy (3), and as such are sufficient to produce bounded estimation error covariance of an unstable process in the case that the state is always transmitted. In contrast to [6], we do not restrict ourselves to the case $\mu_e < \mu$. We show in the below that our encoding scheme provides a measure of secrecy even in the case where the legitimate estimator has a less reliable channel than the eavesdropper. To achieve state secrecy, including to cause an eavesdropper to have an unbounded estimation error covariance, we are unable just to transmit the state estimate at every time instance, motivating our encoding scheme.

B. Encoding Mechanism

Our proposed encoding scheme for the packet z_k is

$$z_k = \begin{cases} x_k, & \nu_k = 0 \\ x_k - Ax_{k-1} + \chi_k, & \nu_k = 1 \end{cases} \tag{4}$$

for $k \geq 1$ and $z_0 = x_0$, where the sensor transmits either the current state or a single step innovation with relation to the previous state encoded by additive noise χ_k. In each packet, we only transmit the information, not the encoding values, making decoding challenging for a potential adversary. The encoding ν_k and χ_k are pre-arranged at the sensor and legitimate estimator. We design the scheduling sequence ν_k and encoding noises χ_k such that each packet z_k appears, at least in a statistical sense, to be the current state value x_k.

To balance legitimate estimator estimation performance with state secrecy against eavesdroppers, several partial encoding schemes have been proposed [9], [12], [32]. These transmission schemes balance providing a reliable estimate to the legitimate estimator encoding while obfuscating from an adversary. As the legitimate estimator estimation performance can decrease, such as from a reduction in shared information [6], quantization encoding [12] or adversary attacks [9], it is often necessary to send the actual state value in some of the packets. The challenge becomes to cleverly balance the trade-off in the encoding scheme, between estimation performance and state secrecy against an eavesdropper.

[2] The spectral radius of a matrix is defined as the maximum absolute eigenvalue $\rho(M) = \max_i |\lambda_i(M)|$ where λ_i is the ith eigenvalue of M.

In our encoding scheme, we propose that the scheduling sequence ν_k and additive encoding noise χ_k for $k \geq 1$ are chosen to be random. The probability distributions and pseudo-random seeds are shared between the transmitter and legitimate estimator in initialization, while the eavesdropper has no knowledge. As such, the realization of the sequence of ν_k and χ_k become pre-arranged, and are known exactly to the transmitter and legitimate estimator but unknown to an eavesdropper. The idea of a pre-arranged distribution seed or common encoding key has been commonly used in several information security facets, such as in watermarking [20], [35] and cryptographic encryption with public and private keys [33], [34] as well as applications to transmission encoding schemes [32].

We choose the distribution of the additive encoding noise χ_k to be a zero-mean Gaussian random variable with covariance

$$E[\chi_k \chi_k^\mathsf{T}] = A^k \Sigma_0 (A^k)^\mathsf{T} + \sum_{\ell=0}^{k-2} A^{k-1-\ell} Q (A^{k-1-\ell})^\mathsf{T}, \quad (5)$$

and χ_k is uncorrelated from the process x_0 and w_k for all k, and χ_k and χ_ℓ for $k \neq \ell$ are uncorrelated. Under this choice of distribution[3], the first and second moments of each packet z_k are equivalent to the state x_k such that $E[z_k] = E[x_k]$ and $E[z_k z_k^\mathsf{T}] = E[x_k x_k^\mathsf{T}]$, for $k \geq 1$. We obtain (5) by computing the expected covariance of the packet in (4) and ensuring the same statistical property for $\nu_k = 0$ and $\nu_k = 1$. An eavesdropper performing a statistical test using the first or second moment would be unable to identify whether each packet z_k is the state x_k or something else. An eavesdropper directly using the packet z_k as the state estimate would have a poor estimate of the true process state.

We choose the distribution of the scheduling sequence ν_k to be a Bernoulli random variable with probability of sending the state as

$$\mathbb{P}(\nu_k = 0) = \mu_d,$$

and encoded innovation as $\mathbb{P}(\nu_k = 1) = 1 - \mu_d$. The probability μ_d is a design variable of our encoding scheme, which trades off nominal estimation performance of the legitimate estimator where the state is sent at every time instance, against secrecy of state information. In the case $\mu_d = 1$ only the state measurement $\nu_k = 0$ is transmitted, while in the case $\mu_d = 0$ only innovations are sent. We bound μ_d between these extremes, $0 < \mu_d < 1$, such that some of the transmissions are innovations and some are the state. We provide guidance in Section VI-A on choice of μ_d in relation to our notions of secrecy and the expected estimation error covariance of the legitimate estimator and eavesdropper.

IV. STATE ESTIMATION PERFORMANCE

In this section, we present the expected performance of the legitimate estimator's state estimate.

A. State Estimator

The MMSE estimate of the state is defined as the expectation of the state given the information received. We define the MMSE prediction of the state as the expectation of the state given the information available at the previous time instance $\hat{x}_{k|k-1} = E[x_k|\mathcal{I}_{k-1}]$. The associated estimation error covariance is denoted as $P_{k|k-1}$.

From [40, Chapter 2] the state estimate update equation is

$$\hat{x}_{k|k} = \hat{x}_{k|k-1} + \gamma_k \Sigma_{k,xz} \left(\Sigma_{k,zz}\right)^{-1} (z_k - \hat{z}_k), \quad (6)$$

with associated estimate covariance update

$$P_{k|k} = \Sigma_{k,xx} - \gamma_k \Sigma_{k,xz} \left(\Sigma_{k,zz}\right)^{-1} \Sigma_{k,zx}, \quad (7)$$

where the expected packet is $\hat{z}_k = E[z_k|\mathcal{I}_{k-1}]$ and the auxiliary variables are

$$\operatorname{Cov}\left(\begin{bmatrix} x_k \\ z_k \end{bmatrix} \middle| \mathcal{I}_{k-1} \right) = \begin{bmatrix} \Sigma_{k,xx} & \Sigma_{k,xz} \\ \Sigma_{k,zx} & \Sigma_{k,zz} \end{bmatrix},$$

where $\Sigma_{k,xx} = P_{k|k-1}$, $\Sigma_{k,zz} = E[(z_k - \hat{z}_k)(z_k - \hat{z}_k)^\mathsf{T}|\mathcal{I}_{k-1}]$, and $\Sigma_{k,xz} = \Sigma_{k,zx}^\mathsf{T} = E[(x_k - \hat{x}_{k|k-1})(z_k - \hat{z}_k)^\mathsf{T}|\mathcal{I}_{k-1}]$.

As the pre-arranged scheduling sequence ν_k and additive noise χ_k are known to the legitimate estimator and the transmitter, the legitimate estimator's expected packet is

$$\hat{z}_k = \begin{cases} E[x_k|\mathcal{I}_{k-1}], & \nu_k = 0 \\ E[x_k - Ax_{k-1}|\mathcal{I}_{k-1}] + \chi_k, & \nu_k = 1 \end{cases}. \quad (8)$$

The MMSE state estimate of the legitimate estimator is

$$\hat{x}_{k|k} = \begin{cases} A\hat{x}_{k-1|k-1}, & \text{when} \quad \gamma_k = 0 \\ x_k, & \text{when} \quad (\gamma_k, \nu_k) = (1,0) \\ x_k - A(x_{k-1} - \hat{x}_{k-1}), & \text{when} \ (\gamma_k, \nu_k) = (1,1) \end{cases}.$$

The following theorem gives the covariance in the three possible outcomes: a dropout occurs, the state is successfully received, and an innovation is successfully received.

Theorem 4.1: The covariance of the legitimate estimator's state estimate is

$$P_{k|k} = \begin{cases} AP_{k-1|k-1}A^\mathsf{T} + Q, & \text{when} \quad \gamma_k = 0 \\ 0, & \text{when} \quad (\gamma_k, \nu_k) = (1,0) \\ AP_{k-1|k-1}A^\mathsf{T}, & \text{when} \quad (\gamma_k, \nu_k) = (1,1) \end{cases}.$$

The proof is direct through application of the dynamics (1) and definition of the expectation operator [40]. The proof can be found in [39].

Inspecting the estimation error covariance of the legitimate estimator in Theorem 4.1, we observe the following.

In the case that the transmission is dropped, $\gamma_k = 0$, the estimation error covariance is the prediction error covariance. This is the worst case as the estimation error builds by a factor of $\rho(A^2)$ and linearly by the driving noise Q.

In the case that the innovation is received $(\gamma_k, \nu_k) = (1,1)$, the estimation error grows by a factor of $\rho(A^2)$, which provides more information about the current state than a dropout. Where the previous state is known exactly and $P_{k-1|k-1} = 0$, then the estimation error covariance remains zero. The encoded innovation provides useful information to the legitimate receiver while the random additive hinders a potential eavesdropper.

[3] See [39] for derivation.

Finally, in the case that the current state is received $(\gamma_k, \nu_k) = (1, 0)$, the estimation error of the current state, $\hat{x}_{k|k}$, is zero as the state is received exactly.

Remark 4.2: MMSE state estimate and associated covariances can alternatively be derived using the Kalman filter. In the case of noisy measurements, the Kalman filter can be employed to provide similar MMSE estimates. While the above result apply in principle, the estimation error covariance in the case of a state receipt would not reduce to exactly zero due to the presence of measurement noise.

B. Expected Performance

The estimation error of the legitimate estimator given in Theorem 4.1, is dependent on the dynamics and the information available at the current time step $\mathcal{I}_k$: scheduling sequence ν_k, additive noise χ_k, and the dropout channel γ_k. We utilize the stochastic properties of the channel environment and scheduling sequence to give the expectation of the legitimate estimator estimation error performance.

To ensure a bounded estimation error covariance at the legitimate estimator, the probability of receiving the state estimate $\mathbb{P}(\gamma_k = 1, \nu_k = 0) = \mu\mu_d$ must be bounded

$$1 - \mu\mu_d < \frac{1}{\rho(A)^2}. \tag{9}$$

The bound in (9) follows the bound in (3) from [38] that the probability of dropouts is bounded by the inverse of the square of the spectral radius of the dynamics. Given a channel quality μ and dynamics A, the minimum choice of design variable is

$$\frac{1}{\mu}\left(1 - \frac{1}{\rho(A)^2}\right) < \mu_d. \tag{10}$$

For $\mu_d < 1$, a better quality channel than (3), where only the state estimate is transmitted, is required.

In the case that the choice of μ_d does not satisfy (9) then $E[P_{k|k}]$ is unbounded, otherwise we have the following result.

Theorem 4.3: The expected estimation error covariance of the legitimate estimator satisfies $\lim_{k\to\infty} E[P_{k|k}] = (1-\mu)S$ where the choice of μ_d satisfies (10), and S is the unique stabilizing solutions to the Lyapunov Equation

$$S = \left(\sqrt{1-\mu\mu_d}A\right) S \left(A^{\mathsf{T}}\sqrt{1-\mu\mu_d}\right) + Q. \tag{11}$$

Proof: See Appendix A. ■

The proof of Theorem 4.3 is shown by considering the expectation of $P_{k|k}$ as the sum of the conditional expectation of $P_{k|k}$ given the outcomes from Theorem 4.1 by the probability of that outcome. Each conditional expectation of $P_{k|k}$ can be written as a function of the expectation of the previous estimation error covariance $P_{k-1|k-1}$ by application of Theorem 4.1. Expanding from time $k-1$ to the initial time $k = 0$, the expectation of $P_{k|k}$ can be written as a function of the initial condition Σ_0 and a sum to time k of the dynamics A and Q and outcome probabilities, comprised of the channel quality μ and design variable μ_d. As $k \to \infty$, we observe that the expression can be written as a converging Lyapunov equation providing the form given in Theorem 4.3.

An alternative proof approach is to consider that as $k \to \infty$, the outcomes of the legitimate estimator form a countably infinite Markov Chain (MC), see [39]. From every state in the MC, the estimation error covariance will return to a zero state when the state estimate is successfully received, such that all states in the MC are reachable. The expectation of $P_{k|k}$ is then the sum of all of the possible MC states multiplied by the limiting distribution of the MC, or the probability of being in a state.

Inspecting the result of Theorem 4.3, we observe that the expectation of the estimation error covariance of the legitimate estimator is a function of the dynamics A and Q, the channel μ, and the encoding scheme with design variable μ_d. The performance is reduced compared to the nominal remote state estimator that transmits the state estimate every time instance[4], or the case that $\mu_d = 1$. Our encoding scheme trades this nominal performance of only sending the state, with secrecy of the state information. Using knowledge of the channel quality and dynamics, the design variable μ_d can be tuned to achieve a certain level of expected estimation error while also ensuring a bounded state estimate. We provide guidance on our encoding design μ_d for secrecy against an eavesdropper in Section VI-A to balance performance of the legitimate estimator against secrecy to an eavesdropper.

V. EAVESDROPPER ESTIMATION PERFORMANCE

We pose our secrecy encoding scheme in the context of a class of adversarial eavesdropper that does not have knowledge of the encoding scheme. The class of eavesdropper directly uses any packets that it *believes* are the state. This amounts to *correctly* using the state in the case $\nu_k = 0$, but *incorrectly* using an encoded innovation as the state in the case $\nu_k = 1$. We limit our analysis to this class of eavesdropper, as even in the situation that an adversary was aware that the innovation was encoded in some of the packets, without knowledge of the additive noise χ_k the eavesdropper would be unable to extract and utilize the innovation.

As the packets are statistically equivalent to the state process, in the sense of the first and second moments, we pose three types of eavesdropper. We consider: a naive eavesdropper that assumes every received packet is the state; a suspicious eavesdropper that suspects not every packet is the state, and has a random chance at guessing the packet type; and a smart eavesdropper that has perfect packet identification, and correctly uses the state and discards the innovation.

In this section, we show the expectation of the estimation error covariance of the class of eavesdropper, and for each type of eavesdropper compare to the legitimate user's performance. We then provide an approach to choose an appropriate design variable μ_d, and a numerical illustration.

A. Expected Eavesdropper Estimation Performance

At the receipt of each packet z_k, we consider that the eavesdropper may perform a test on the packet to make a

[4] This can be shown by utilizing the monotonicity property of the Lyapunov equation given in Lemma 5.7 below.

choice whether to utilize or discard the packet. Let us define $b_k = 1$ as the case where the eavesdropper identifies a received packet z_k as the state and uses the packet, and $b_k = 0$ as the case where the eavesdropper identifies a received packet z_k as not the state and so discards the packet. Let us define the eavesdropper's belief to use a packet as the posterior probability test conditioned on the received packet as $\mathbb{P}(b_k = 1 | z_k, \gamma_k^e, \nu_k)$, and the belief to discard a packet as $\mathbb{P}(b_k = 0 | z_k, \gamma_k^e, \nu_k) = 1 - \mathbb{P}(b_k = 1 | z_k, \gamma_k^e, \nu_k)$. We outline in the following sections how each type of eavesdropper forms these conditional probabilities.

An eavesdropper has five possible events: successfully receives a state which it *correctly* uses $(\gamma_k^e, \nu_k, b_k) = (1,0,1)$ or incorrectly discards $(\gamma_k^e, \nu_k, b_k) = (1,0,0)$, successfully receives an innovation which it *incorrectly* uses $(\gamma_k^e, \nu_k, b_k) = (1,1,1)$ or correctly discards $(\gamma_k^e, \nu_k, b_k) = (1,1,0)$, or the packet is dropped $(\gamma_k^e = 0)$. As discarding a successfully received packet (cases $b_k = 0$) is equivalent to dropping the packet $(\gamma_k^e = 0)$, the five events reduce to three outcomes.

First: successfully receiving a state which the eavesdropper correctly uses; probability $p_r^e = \mathbb{P}(\gamma_k^e = 1, \nu_k = 0, b_k = 1)$.

Second: successfully receiving an innovation which the eavesdropper incorrectly uses as the state, with probability $p_i^e = \mathbb{P}(\gamma_k^e = 1, \nu_k = 1, b_k = 1)$.

Third: the eavesdroppers drops the packet or discards a successfully received packet which it believes is not the state, with probability $p_d^e = \mathbb{P}(\gamma_k^e = 0) + \mathbb{P}(\gamma_k^e = 1, \nu_k = 0, b_k = 0) + \mathbb{P}(\gamma_k^e = 1, \nu_k = 1, b_k = 0)$.

The state estimate of an eavesdropper is

$$\hat{x}_k^e = \begin{cases} A\hat{x}_{k-1}^e, & \text{when} \quad (\gamma_k^e = 0) \text{ or } (\gamma_k^e, \nu_k, b_k) = (1,0,0) \\ & \qquad \text{or } (\gamma_k^e, \nu_k, b_k) = (1,1,0) \\ x_k, & \text{when} \quad (\gamma_k^e, \nu_k, b_k) = (1,0,1) \\ x_k - Ax_{k-1} + \chi_k, & \text{when} \quad (\gamma_k^e, \nu_k, b_k) = (1,1,1) \end{cases}$$

where the predicted estimate uses dynamics, and a successfully received packet is used directly. We derive the covariance of the state estimate similar to Theorem 4.1, then follow a similar argument as Theorem 4.3 for the expectation of the estimation error covariance.

Lemma 5.1: The eavesdropper's estimation error covariance is

$$P_{k|k}^e = \begin{cases} AP_{k-1|k-1}^e A^\mathsf{T} + Q, \quad \text{when} \quad (\gamma_k^e = 0) \\ \qquad \text{or } (\gamma_k^e, \nu_k, b_k) = (1,0,0) \\ \qquad \text{or } (\gamma_k^e, \nu_k, b_k) = (1,1,0) \\ 0, \quad \text{when} \quad (\gamma_k^e, \nu_k, b_k) = (1,0,1) \\ 2\left(A^k \Sigma_0 (A^k)^\mathsf{T} + \sum_{\ell=0}^{k-2} A^{k-1-\ell} Q (A^{k-1-\ell})^\mathsf{T}\right), \\ \qquad \text{when} \quad (\gamma_k^e, \nu_k, b_k) = (1,1,1) \end{cases}$$

The proof is direct through application of the dynamics (1), definition of the expectation operator [40], and the encoding scheme (4). The proof can be found in [39].

Critically, while we can quantify in Lemma 5.1 the estimation error covariance of an eavesdropper using knowledge of the mismatch between the encoding scheme and the eavesdropper's assumption, this would be unknown to the eavesdropper. The eavesdropper assumes that upon receiving a packet $(\gamma_k^e = 1)$ and utilizing the packet $(b_k = 1)$ their estimation error covariance is zero, which would not be the case upon receiving an innovation. From Lemma 5.1, we note that upon receipt and use of an innovation, the estimation error covariance is instead a function of the dynamics and time k.

Theorem 5.2: The expectation of the estimation error covariance of the eavesdropper is

$$E[P_{k|k}^e] = (p_d^e)^k A^{k-1} \Sigma_0 (A^{k-1})^\mathsf{T} + \sum_{\ell=0}^{k-1} (p_d^e)^{\ell+1} A^\ell Q (A^\ell)^\mathsf{T}$$
$$+ p_i^e 2 \sum_{\ell=0}^{k-1} (p_d^e)^\ell \left(A^k \Sigma_0 (A^k)^\mathsf{T} + \sum_{j=0}^{k-\ell-2} A^{k-1-j} Q (A^{k-1-j})^\mathsf{T}\right),$$

where p_i^e is the probability of receiving and utilizing an innovation, and p_d^e is the probability of dropping or discarding a packet.

Proof: See Appendix B. ■

Inspecting the result of Theorem 5.2, we note that the expectation of the eavesdropper's estimation error covariance is a function of the dynamics A and Q, the initial state covariance Σ_0, the time k, and the probability of incorrectly using an innovation p_i^e and probability of dropping or discarding a packet p_d^e. The probability of use or discard of encoded innovation packets depend on the belief that a received packet is the state. We now distinguish the class of eavesdropper through three types of packet analysis techniques. For each class, we utilize the result of Theorem 5.2 to compare to the legitimate estimator's performance in the sense of our definitions of secrecy.

B. Naive Eavesdropper

Consider a naive eavesdropper that assumes that every packet transmitted to the legitimate estimator is the state, $\hat{z}_k = x_k$ for all k. Performing basic statistical tests, such as computing the first or second moment on each received packet z_k, the naive eavesdropper would be unable to identify a difference between state packets $(\nu_k = 0)$ and innovation packets $(\nu_k = 1)$, as by design $E[z_k] = E[x_k]$, see Section III-B. The eavesdropper's belief whether to use a packet that is successfully received is $\mathbb{P}(b_k = 1 | z_k, \gamma_k^e = 1, \nu_k) = 1$, irrespective of the packet containing the state $(\nu_k = 0)$ or innovation $(\nu_k = 1)$. The probability of the naive eavesdropper using the state or innovation are then $p_r^e = \mathbb{P}(\gamma_k^e = 1, \nu_k = 0, b_k = 1) = \mu_e \mu_d$, $p_i^e = \mathbb{P}(\gamma_k^e = 1, \nu_k = 1, b_k = 1) = \mu_e(1 - \mu_d)$, and probability of packet drop or discard is $p_d^e = 1 - \mu_e$.

We state the estimation error performance of the naive eavesdropper from the result in Theorem 5.2.

Corollary 5.3: The expectation of the estimation error covariance of the naive eavesdropper diverges, $E[P_{k|k}^e] \to \infty$ as $k \to \infty$, satisfying condition (ii) of Definition 2.

Proof: See Appendix C. ■

As the naive eavesdropper treats all received packets as the state, it will inadvertently use the innovation packets which significantly degrades the naive eavesdropper's state estimate. The result of Corollary 5.3 gives that the expectation of the estimation error covariance is a function of time k

with some terms diverging as k increases. We note that the diverging terms in the expected performance are larger for larger probabilities p_i^e, or smaller μ_d. Thus while any choice of μ_d that satisfies (9) will ensure perfect secrecy, a smaller μ_d will provide faster divergence of the naive eavesdropper's estimate. Additionally, we observe that even in the case of a perfect channel $\mu_e = 1$ and $p_d^e = 0$, the naive eavesdropper's expected performance still diverges.

C. Suspicious Eavesdropper

Consider an eavesdropper that becomes suspicious that not all of the received packets are the state. This suspicious eavesdropper applies a statistical test to each packet that it receives to form a belief of whether to use the packet or to discard. Such analysis could be performed by testing the sequence of received packet $\mathcal{I}_k^e$, using online statistical techniques such as Quickest Change Detection [17], [20].

As this eavesdropper is performing a statistical test on the content of the received packet z_k, the posterior probability to use the packet would be correlated with the value of that packet and thus the encoding ν_k and χ_k. For simplicity in analysis, we assume that the eavesdropper has a fixed random chance of correctly identifying a packet upon receipt, independent of the packet value, encoding, or previous test outcome. As such, our assumption is that the probability of belief is i.i.d. and uncorrelated from the packet z_k. While a major simplifying assumption, this permits the below result, which gives an indication to the potential eavesdropper performance in the situation of non-perfect statistical tests. In the following section, we analyze a smart eavesdropper that has perfect detection through statistical analysis of received packets.

Let us define the probability for the eavesdropper to use a packet that contains the state as $\mathbb{P}(b_k = 1|z_k, \gamma_k^e = 1, \nu_k = 0) = \mu_b$, and to use a packet that contains the innovation as $\mathbb{P}(b_k = 1|z_k, \gamma_k^e = 1, \nu_k = 1) = \bar{\mu}_b$, where $0 < \mu_b < 1$ and $0 < \bar{\mu}_b < 1$. The naive and smart eavesdropper operate at the boundaries of μ_b and $\bar{\mu}_b$. The naive eavesdropper utilizes all packets regardless of encoding type then $\mu_b = \bar{\mu}_b = 1$. The smart eavesdropper perfectly identifies the packet type such that $\mu_b = 1$ and $\bar{\mu}_b = 0$. In practice, if the outcomes at an eavesdropper were accessible, the parameters μ_b and $\bar{\mu}_b$ could be computed post-experiment by assuming all decision events were independent. For μ_b the computation would involve dividing the total number of successful decisions $b_k = 1$ conditioned on the event $(\gamma_k^e = 1, \nu_k = 0)$ by the total number of instances that the event $(\gamma_k^e = 1, \nu_k = 0)$ occurred. By the independence assumption, the probability of the suspicious eavesdropper using the state or innovation are then $p_r^e = \mathbb{P}(\gamma_k^e = 1, \nu_k = 0, b_k = 1) = \mu_e\mu_d\mu_b$, $p_i^e = \mathbb{P}(\gamma_k^e = 1, \nu_k = 1, b_k = 1) = \mu_e(1-\mu_d)\bar{\mu}_b$, and the probability to drop or discard a packet is $p_d^e = 1 - \mu_e\mu_d\mu_b - \mu_e\bar{\mu}_b + \mu_e\mu_d\bar{\mu}_b$. The above probabilities are a consequence of the assumption that the channel quality, schedule to transmit the state, and eavesdropper belief, are i.i.d. random variables and uncorrelated from each other and the process.

We state the estimation error performance of the suspicious eavesdropper from the result in Theorem 5.2.

Corollary 5.4: The expectation of the estimation error covariance of the suspicious eavesdropper diverges, $E[P_{k|k}^e] \to \infty$ as $k \to \infty$, satisfying condition (ii) of Definition 2.

Proof: See Appendix C. ■

As the suspicious eavesdropper has a random chance of incorrectly identifying encoded innovation packets as the state, it will inadvertently use these packets which significantly degrades its state estimate. The result of Corollary 5.4 gives that the expectation of the estimation error covariance is a function of time k with some terms diverging as k increases.

In contrast to the naive eavesdropper's expected estimation error covariance, see Corollary 5.3, the probability of using an innovation, p_i^e, is smaller $\mu_e(1-\mu_d) \geq \mu_e(1-\mu_d)\bar{\mu}_b$, for $\bar{\mu}_b < 1$, but the probability of the dropout, p_d^e, is much larger. For some choices of the eavesdropper's beliefs μ_b and $\bar{\mu}_b$ the expectation of the suspicious eavesdropper's performance will be worse than for the naive eavesdropper.

Remark 5.5: Consider the scenario where the suspicious eavesdropper correctly identifies all packets that contain the state, such that $\mu_b = 1$ but makes errors on the innovation packets such that $\bar{\mu}_b > 0$ and $p_i^e > 0$. By Corollary 5.4 the expectation of the eavesdropper's estimation error covariance will diverge. We note that for errors in identification of the encoded innovations such that the eavesdropper uses these packets will diverge the eavesdropper's estimate.

D. Smart Eavesdropper

Consider a smart eavesdropper that analyses the packets, but in contrast to the suspicious eavesdropper has perfect performance. The smart eavesdropper perfectly identifies all received packets that are the state measurement $\mathbb{P}(b_k = 1|z_k, \gamma_k^e = 1, \nu_k = 0) = 1$, and uses these packets. The smart eavesdropper perfectly identifies all received packets that are not the state $\mathbb{P}(b_k = 1|z_k, \gamma_k^e = 1, \nu_k = 1) = 0$, and discards these packets. Effectively, the smart eavesdropper can identify the sequence ν_k. However, we consider that it does not know the realization of χ_k and is unaware of the full encoding mechanism (4), so cannot decode the innovations. We consider that it would be challenging for an eavesdropper to identify the value of χ_k inside the packet z_k as the random variable is independent and uncorrelated from the state process x_k and scheduling sequence ν_k.

The probability of the smart eavesdropper using the state or innovation is $p_r^e = \mathbb{P}(\gamma_k^e = 1, \nu_k = 0, b_k = 1) = \mu_e\mu_d$, $p_i^e = \mathbb{P}(\gamma_k^e = 1, \nu_k = 0, b_k = 1) = 0$, and probability of packet drop or discard is $p_d^e = 1 - \mu_e\mu_d$.

We note that the second outcome introduced in Section V-A is eliminated. We note that this is the best type of eavesdropper in the class that we analyze. For an eavesdropper to obtain better performance, an adversary would need to decode the innovation, which is outside of the class that we consider.

The smart eavesdropper effectively functions as a remote state estimator where the state is transmitted every time instance with a channel quality of $p_r^e = \mu_e\mu_d$. This result is a consequence of our encoding scheduling sequence ν_k being i.i.d. and uncorrelated to the eavesdropper's channel. Following [38], a necessary and sufficient condition for the smart eavesdropper to have a bounded estimation error covariance, is that the encoding design probability is upper bounded by

$$\frac{1}{\mu_e}\left(1-\frac{1}{\rho(A)^2}\right) < \mu_d. \tag{12}$$

The result of Lemma 5.1 can be reduced by noting that the case $(\gamma_k^e, \nu_k, b_k) = (1,1,1)$ is discarded. The state estimate of the smart eavesdropper is

$$\hat{x}_k^e = \begin{cases} A\hat{x}_{k-1}^e, & \text{when } \gamma_k^e = 0 \text{ or } (\gamma_k^e, \nu_k) = (1,1) \\ & \text{or } (\gamma_k^e, \nu_k, b_k) = (1,0,0) \\ x_k, & \text{when } \ (\gamma_k^e, \nu_k, b_k) = (1,0,1) \end{cases}$$

with covariance

$$P_{k|k}^e = \begin{cases} AP_{k-1|k-1}^e A^\mathsf{T} + Q, \\ \quad \text{when } \ \gamma_k^e = 0 \text{ or } (\gamma_k^e, \nu_k) = (1,1) \\ \quad \text{or } (\gamma_k^e, \nu_k, b_k) = (1,0,0) \\ 0, \quad \text{when } \ (\gamma_k^e, \nu_k) = (1,0) \end{cases}$$

This can be shown directly from [40] and is simpler than the state estimate of the legitimate estimator, see Theorem 4.1. Unlike the naive and suspicious eavesdroppers above, the smart eavesdropper can correctly quantify its own estimation error covariance, $P_{k|k}^e$, as it is aware of the nature of the packets it is using.

To compare the performance of the smart eavesdropper to the legitimate estimator, we establish the expectation of the estimation error covariance of the smart eavesdropper. In the case that μ_e or μ_d do not satisfy (12), then $E[P_{k|k}^e]$ is unbounded. In the case that μ_e and μ_d satisfy (12) then we have the following result.

Lemma 5.6: The expectation of the estimation error covariance of the smart eavesdropper satisfies $\lim_{k\to\infty} E[P_{k|k}^e] = (1-\mu_e\mu_d)S^e$ where μ_e and μ_d satisfy (12), and S^e is the unique stabilizing solution to the Lyapunov Equation

$$S^e = \left(\sqrt{1-\mu_e\mu_d}A\right) S^e \left(A^\mathsf{T}\sqrt{1-\mu_e\mu_d}\right) + Q. \tag{13}$$

The proof follows that of Theorem 4.3 and Theorem 5.2, but is simpler as the eavesdropper has only two possible channel outcomes. As $p_i^e = 0$ for the smart eavesdropper, then the diverging terms in Theorem 5.2 are removed, and the expectation then converges. The proof can be found in [39].

To show secrecy as a function of design variable μ_d and channel qualities, μ and μ_e, we give the following monotonicity result of the Lyapunov equation.

Lemma 5.7: Consider a $\beta, \beta^\star$ where $0 < \beta, \beta^\star < 1$, $\rho(\sqrt{1-\beta}A) < 1$ and $\rho(\sqrt{1-\beta^\star}A) < 1$ and introduce the following two Lyapunov equations

$$W = \sqrt{1-\beta}AWA^\mathsf{T}\sqrt{1-\beta} + Q, \tag{14}$$

$$W^\star = \sqrt{1-\beta^\star}AW^\star A^\mathsf{T}\sqrt{1-\beta^\star} + Q, \tag{15}$$

where W and $W^\star$ are the unique stabilizing solutions. In the case that $\beta^\star < \beta$ then trace $W <$ trace $W^\star$.

Proof: See Appendix D. ■

Using Lemmas 5.6 and 5.7 and Theorem 4.3, we compare the expected estimation error of the smart eavesdropper against the legitimate estimator. The differences in performance are related to the difference in channel qualities, and scheduling sequence design. We explore the cases where the eavesdropper channel quality is worse than, or equal to, the legitimate estimator's channel quality.

Theorem 5.8: In the case that the eavesdropper has a worse or equal quality channel to the legitimate estimator, $\mu_e \le \mu$ and the scheduling sequence is chosen in the range

$$\frac{1}{\mu_e}\left(1-\frac{1}{\rho(A)^2}\right) < \mu_d < 1, \tag{16}$$

then the trace of the expected estimation error of the legitimate estimator is strictly less than the eavesdropper trace $E[P_{k|k}] <$ trace $E[P_{k|k}^e]$. This satisfies condition (ii) of Definition 1.

Proof: Recall (10), Theorem 4.3 and Lemma 5.6. For any $\mu_d < 1$ and $\mu_e \le \mu$ then $1-\mu < 1-\mu_e\mu_d$. In the case $\mu_e = \mu$ then $S \equiv S^e$. In the case $\mu_e < \mu$, let $\beta = \mu\mu_d$ and $\beta^\star = \mu_e\mu_d$ and via Lemma 5.7, trace $S <$ trace S^e. It follows in both cases that $(1-\mu)$trace $S < (1-\mu_e\mu_d)$trace S^e. ■

From Theorem 5.8, we can conclude that our encoding scheme achieves a level of relative secrecy against the smart eavesdropper that has an equal or worse channel quality. For scenarios where the smart eavesdropper has a better quality channel than the legitimate estimator, $\mu_e > \mu$, there may exist a bound on μ_d where our encoding scheme provides relative secrecy. We explore this numerically in the following section.

Additionally, we notice that the expected estimation error covariances for the legitimate estimator and smart eavesdropper given in Theorem 4.3 and Lemma 5.6, respectively, hold for stable processes where $\rho(A) < 1$. Relative secrecy shown in Theorem 5.8 follows as a result. We further explore stable processes in [41].

In the case where the eavesdropper has a strictly worse quality channel and the dynamics are unstable such that $\rho(A) > 1$, we observe an extension to Theorem 5.8.

Theorem 5.9: In the case that $\mu_e < \mu$, and the dynamics are unstable $\rho(A) > 1$, the smart eavesdropper's expected state estimate is unbounded $E[P_{k|k}^e] \to \infty$ while the legitimate estimator's estimate is bounded where the design variable μ_d is bounded by

$$\frac{1}{\mu}\left(1-\frac{1}{\rho(A)^2}\right) < \mu_d \le \frac{1}{\mu_e}\left(1-\frac{1}{\rho(A)^2}\right). \tag{17}$$

This satisfies condition (ii) of Definition 2.

Proof: Choice of μ_d satisfying (10) to ensure a bounded estimate for the legitimate estimator informs the lower bound. Failing (12) such that the eavesdropper has an unbounded estimation error covariance informs the upper bound. ■

The proof of Theorem 5.9 relies on the minimum bounds for a valid remote state estimate as drawn from (10) and (12). In the scenario that the smart eavesdropper's channel quality is equal or better than the legitimate user $\mu \ge \mu_e$, or the dynamics are marginally stable $\rho(A) = 1$, then the bounding range of μ_d in (17) cannot be formed.

Comparing the result of Theorem 5.9 to the proposal of [6] the bound on the random transmission of the state is similar to achieve perfect secrecy. However, our encoder is different as we transmit an encoded innovation instead of no information, which the legitimate estimator can decode, providing better legitimate estimation performance while still ensuring secrecy of the state estimate against an eavesdropper.

Under a channel model with signal fading over distance, we might expect the case of eavesdropper channel quality worse than the legitimate estimator to be more common, as a stealthy eavesdropper might be physically located further away from the transmitter as considered in [6].

We observe from the results of Theorems 5.8 and 5.9, that through the use of the innovations in our encoder design, the legitimate estimator has lower expectation of estimation error covariance than a smart eavesdropper and thus a better state estimate in the case of better or the same channel quality. Our proposed encoding technique is most beneficial in the case where the legitimate user has a better or equal channel quality to the eavesdropper.

VI. Scheduling Sequence Design for Secrecy

We now discuss approaches to determine an appropriate design variable μ_d to generate the scheduling sequence, and provide a numerical illustration. Let us briefly recall our packet encoding from (4)

$$z_k = \begin{cases} x_k, & \nu_k = 0 \\ x_k - Ax_{k-1} + \chi_k, & \nu_k = 1 \end{cases}$$

for $k \geq 1$ and $z_0 = x_0$, and we randomize transmission of the state with $\mathbb{P}(\nu_k = 0) = \mu_d$, and χ_k is a zero-mean Gaussian random variable designed such that the first and second moment of the packet are the same as the state.

A. Scheduling Distribution Design

Consider a given dynamics A and Q, and legitimate estimator channel quality μ and eavesdropper channel quality μ_e, then the expectations of the estimation error covariance can be written as a function of μ_d. The expectation of the estimation error covariance of the legitimate estimator from Theorem 4.3 can be written as

$$J(\mu_d) = \text{trace } E[P_{k|k}] = (1-\mu)\text{trace } S, \tag{18}$$

and the smart eavesdropper from Lemma 5.6

$$J_e(\mu_d) = \text{trace } E[P^e_{k|k}] = (1-\mu_e\mu_d)\text{trace } S^e,$$

where S and S^e are functions of μ_d, see (11) and (13). Before providing a method to select an encoding design μ_d, we observe the following monotonicity result.

Lemma 6.1: The trace of the expectation of the estimation error covariance for the legitimate estimator $J(\mu_d)$ and smart eavesdropper $J_e(\mu_d)$ are monotonically decreasing in μ_d, such that for $\mu_d^\star \leq \mu_d$ then $J(\mu_d) \leq J(\mu_d^\star)$ and $J_e(\mu_d) \leq J_e(\mu_d^\star)$.

Proof: Consider $\mu_d^\star < \mu_d$. Recall Theorem 4.3, and let $\beta = \mu\mu_d$ and $\beta^\star = \mu\mu_d^\star$ then via Lemma 5.7, trace $S <$ trace $S^\star$. Recall Lemma 5.6, and let $\beta^e = \mu_e\mu_d$, $\beta^{e,\star} = \mu_e\mu_d^\star$ then via Lemma 5.7, trace $S^e <$ trace $S^{e,\star}$, and $1-\beta < 1-\beta^\star$. The result follows. ■

The result of Lemma 6.1 gives that as we decrease μ_d towards the minimum value in (10), and as such transmit more innovations, the expectation of the estimation error covariance of both the legitimate estimator and the smart eavesdropper increase. Conversely as we increase μ_d towards 1, such that we transmit fewer innovations, the expectation of the estimation error covariance of both the legitimate estimator and the smart eavesdropper reduces. Our design variable μ_d then trades off the estimation performance of the legitimate estimator for secrecy against the eavesdropper.

We now establish a range on the encoding design μ_d to satisfy the constraints (10) and $\mu_d < 1$ and condition (i) of our secrecy Definitions 1 and 2. Applying the monotonicity result of Lemma 6.1, the minimum choice of μ_d will be at the bound $J(\mu_d) = \Omega$ by a given $\Omega > 0$, while the maximum choice will be at the bound $J(\mu_d) = 0$. The minimum choice that ensures that the expected estimation error covariance of the legitimate estimator is bounded by a given $\Omega > 0$ can be found by maximizing[5] (18) over possible μ_d

$$\mu_d^{\min} = \sup J(\mu_d) < \Omega \text{ such that } \frac{1}{\mu}\left(1 - \frac{1}{\rho(A)^2}\right) < \mu_d < 1,$$

where the lower bound is from (10) to ensure a valid state estimate. The maximum choice can be found by minimizing (18) greater than 0

$$\mu_d^{\max} = \inf J(\mu_d) > 0 \text{ such that } \frac{1}{\mu}\left(1 - \frac{1}{\rho(A)^2}\right) < \mu_d < 1,$$

where the lower bound is from (10) to ensure a valid state estimate. In many scenarios $\mu_d^{\min}$ will be close to the bound given in (10), i.e. the supremum. While, $\mu_d^{\max}$ will be close to the maximum bound 1, i.e. the infimum. A choice in the range $\mu_d^{\min} < \mu_d < \mu_d^{\max}$ ensures condition (i) of Definitions 1 and 2. However, in some situations, the *inf* and *sup* operations on $J(\mu_d)$ can occur as the min and maxvalues (in the sense that μ_d is inside the inequality bounds). The corresponding strict inequality on μ_d choice range can then be non-strict.

For the case $\mu_e \leq \mu$, while any choice of encoding design μ_d in the ranges $\mu_d^{\min} < \mu_d < \mu_d^{\max}$ and (16), from Theorem 5.8, will give secrecy under Definition 1, we may be interested in the encoding design that maximizes the secrecy gain. To maximize the secrecy gain, we desire to find the encoding that achieves the biggest performance difference. Let us introduce a function of the difference in expectation of estimation error covariances

$$\begin{aligned} J_r(\mu_d) &= \text{trace } E[P^e_{k|k}] - \text{trace } E[P_{k|k}] \\ &= (1-\mu_e\mu_d)\text{trace } (S^e) - (1-\mu)\text{trace } S, \end{aligned}$$

where both S^e and S are functions of the design μ_d. We note that $J_r(\mu_d) > 0$ for any μ_d in the range (16), as trace $E[P^e_{k|k}] >$ trace $E[P_{k|k}]$ by Theorem 5.8.

To obtain an encoding design $\mu_d^\star$ that maximizes the estimation error covariance difference, we find the μ_d that maximizes $J_r(\mu_d) > 0$

$$\mu_d^\star = \arg\max J_r(\mu_d) > 0, \tag{19}$$

such that the constraints $\mu_d^{\min} < \mu_d^\star < \mu_d^{\max}$, and (16) hold. The choice of $\mu_d^\star$ for the encoding design will provide the biggest secrecy gain against the smart eavesdropper.

[5] Using any standard constrained nonlinear solver.

In the case of better eavesdropper channel quality $\mu < \mu_e$ there may exist a range on μ_d where our encoding design will satisfy Definition 1. There may exist a value $\mu_d^\star$ that maximizes $J_r(\mu_d) > 0$ from the optimization (19) such that only the constraint $\mu_d^{\min} < \mu_d^\star < \mu_d^{\max}$ is satisfied. Noting that the constraint (16) does not apply in the case $\mu < \mu_e$. If an encoding design $\mu_d^\star$ exists, then there may also be a range $\underline{\mu}_d < \mu_d^\star < \overline{\mu}_d$ that provides $J(\mu_d) > 0$, and can be computed $\underline{\mu}_d = \arg\min J_r(\mu_d) > 0$, with constraint $\mu_d^{\min} < \underline{\mu}_d < \mu_d^\star$ and $\overline{\mu}_d = \arg\min J_r(\mu_d) > 0$, with constraint $\mu_d^\star < \overline{\mu}_d < \mu_d^{\max}$.

Finally, in the case of worse eavesdropper channel quality $\mu_e < \mu$ the best legitimate estimator performance, where the eavesdropper has an unbounded estimate under Definition 2, is given by $\mu_d^{\max} = \arg\min J(\mu_d) > 0$, such that the constraint (17) holds.

B. Numerical Illustration of the Impact of Scheduling Design on Different Relative Channel Qualities

We briefly illustrate the relative performance of the legitimate estimator and smart eavesdropper in a numerical example on different relative channel qualities. We explore the scenarios where the probability of dropout for the smart eavesdropper is larger, the same, and smaller than the legitimate estimator. We do not illustrate the performance of the naive and suspicious eavesdroppers, as via Corollary 5.3 and 5.4 the estimation performance is divergent for any μ_d.

Consider the dynamics in (1) with

$$A = \begin{bmatrix} 1 & 0.3 \\ 0.5 & 1.001 \end{bmatrix}, \text{ and } Q = 10^{-3}\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

where we note that $\rho(A) = 1.3878 > 1$. Consider a channel quality of $\mu = 0.9$ for the legitimate estimator. Using (10) we obtain that the design variable is lower bounded $0.5342 < \mu_d$.

Let us consider four cases of smart eavesdropper channel quality of $\mu_e^1 = 0.85$, $\mu_e^2 = \mu$, $\mu_e^3 = 0.95$, and $\mu_e^4 = 0.99$. Figure 2 shows the absolute difference in the traces of the expected estimation error between the smart eavesdropper and the legitimate estimator $J_r(\mu_d)/J(\mu_d)$, against the encoding design variable μ_d for the four cases.

In the case that the eavesdropper's channel quality is worse ($\mu_e^1 < \mu$ in dotted magenta) or equal ($\mu_e^2 = \mu$ in dashed blue) to the legitimate estimator, the trace of the expected estimation error covariance of the eavesdropper, while bounded, is larger for any choice of valid design. These results illustrate Theorem 5.8 and satisfaction of Definition 1.

For the case where the eavesdropper has a worse quality channel $\mu_e^1 < \mu$, using (17) from Theorem 5.9 encoding designs in the range $0.5342 < \mu_d < 0.5656$ force the smart eavesdropper's estimation error covariance to be unbounded while the legitimate estimator's estimation error covariance remains bounded, achieving Definition 2.

In the case that the eavesdropper's channel quality is better than the legitimate estimator $\mu_e^3 = 0.95$, see the solid black line in Figure 2, there is a visible range of μ_d where $J_r(\mu_d) > 0$. Optimizing (19), the encoding design $\mu_d = 0.5745$ gives the largest positive value of $J_r(\mu_d)$, with the range $0.5342 < \mu_d < 0.8931$ giving $J_r(\mu_d) > 0$. In some scenarios where the eavesdropper has a better quality channel, our encoding design can provide relative secrecy under Definition 1.

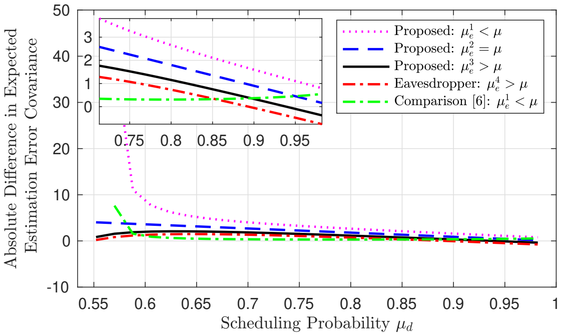

Fig. 2. Comparison of the absolute difference in trace of the expected estimation error covariance of the legitimate estimator with the smart eavesdropper under four channel qualities (worse, equal, better, much better). Eavesdropper with worse channel quality in dotted magenta, equal channel quality in dashed blue, better channel quality in solid black, and much better channel quality in dot-dashed red. The results of Theorem 5.8 are apparent where the eavesdropper has worse performance than the legitimate estimator in the case of worse or equal channel quality. Comparison with transmission design using [6] in the dot-dashed green line.

For a near perfect eavesdropper channel of $\mu_e^4 = 0.99$, a choice of μ_d that provides $J_r(\mu_d) > 0$ is not apparent in Figure 2 (dot-dashed red line). Using (19), the encoding design $\mu_d = 0.5571$ gives the largest positive value of $J_r(\mu_d)$, and the range $0.5342 < \mu_d < 0.9384$ gives $J_r(\mu_d) > 0$. Even in the scenario where an eavesdropper has a significantly better quality channel, our encoding design still provides relative state secrecy under Definition 1.

The proposed secrecy design in [6] is to randomly send either the measurement or no information, with some fixed probability. This design is shown to be secret when the eavesdropper has a strictly worse quality channel than the legitimate estimator. In our proposed design, see (4), we transmit encoded state information instead of no information. This improves the state estimation performance at the legitimate receiver.

The performance of a legitimate estimator utilizing [6] can be described by Lemma 5.6, with channel quality $\mu_e = p_1$ and scheduling probability $\mu_d = p$. The performance gains for the legitimate estimator utilizing our proposed method compared to [6] with the same scheduling probability can be seen by comparing under our proposed method the legitimate estimator and smart eavesdropper with the same channel quality, see the dashed blue line in Figure 2.

Additionally, we compute the relative performance of the eavesdropper and legitimate estimator using the transmission design of [6] for the worse eavesdropper channel $\mu_e^1 < \mu$. This is shown as the dashed green line in Figure 2. The absolute difference in trace of the expected estimation error covariance between the eavesdropper and legitimate estimator operating utilizing the transmission design in [6] results in a smaller difference in relative secrecy, compared to our proposed design in the dotted magenta line.

VII. APPLICATION TO POWER SYSTEMS

We now consider an application of our proposed transmission encoding scheme to a microgrid. A microgrid is a small electricity grid, typically consisting of local generation, such as solar photo-voltaics, and local storage, such as batteries, to supply a small to medium load. The load could include a typical suburban house, several houses, or contained facility such as a hospital [29]. In metropolitan areas, the microgrid can connect to the main grid with import and export capability, while in remote areas, the microgrid is isolated. The interconnection between multiple microgrids and to the main utility grid, enables coordination to achieve global system goals. However, this networking exposes the whole power system to cyber-attacks altering the behavior of the system [42].

With advancements in solar generation and battery storage technology, there has recently been a rise in the microgrid ‘prosumer’ [43]. The ‘prosumer’ both produces electricity and exports to the grid, as well as consumes and imports power from the grid. The challenge of a grid connected microgrid is to control the power flow to either maximize the use of the local storage and minimize purchase of power from the grid, or to maximize the export of power to the grid for profit [44].

While individuals may benefit from maximizing sale of power to the grid, many users in a small geographic area exporting power can cause grid instability [45]. As more consumer households transition to microgrids with local power generation and storage, it becomes necessary for a network operator to monitor and control the connected microgrid to ensure stability [46]. The transmission of consumer data, and behavior as extracted from power flow data poses a privacy risk [47]. This motivates the associated cybersecurity problem to ensure confidentiality of the storage levels and generation potential from eavesdroppers.

To autonomously control the power flows in a connected microgrid, [29] posed a constrained model predictive control design. Their experimental microgrid consisted of a battery and hydrogen storage systems, green power from solar panels, household load, and a grid connection for export for sale and purchase import power. Figure 3 illustrates the power flow connections in this example microgrid.

A. Microgrid Dynamics

The dynamics of the battery and hydrogen storage systems can be parameterized as nonlinear ordinary differential equations. For the purposes of control, [29] introduced a discrete-time linearized model to describe the change in storage charge from the input power flows. The model states are the percentage battery state of charge (SOC) and hydrogen level (LOH) such that $x = [SOC,\ LOH]^\top$, the control inputs are the hydrogen power flow P_H and the grid power flow P_{grid} such that $u = [P_H,\ P_{grid}]$, while the green power P_{solar}, and load P_{load}, are considered uncontrolled input disturbances. The power to the battery storage is the sum of all power flows by Kirchhoff’s laws $P_{bat} = P_{load} - P_{solar} - P_H - P_{grid}$. All power flows are in kW. The discrete-time linearized dynamics posed in [29] are

$$x_{k+1} = Ax_k + Bu_k + B_d(P_{solar} - P_{load}), \tag{20}$$

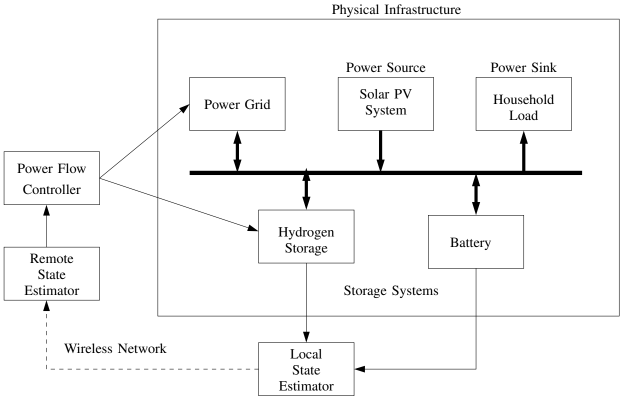

Fig. 3. Illustration of the microgrid power flow connections, adapted from [29]. Local green power supplies a small to medium sized load, such as a house, with batteries and hydrogen system providing power storage. The controller manages the power flows to maximize the use of the storage systems and minimize purchase of power from the grid.

where the sampling rate is 1 second, A is the identity matrix of size 2×2 and

$$B = \begin{bmatrix} 1.56 & 1.56 \\ -5.66 & 0 \end{bmatrix} \times 10^{-3}, \quad B_d = \begin{bmatrix} 1.56 \\ 0 \end{bmatrix} \times 10^{-3}.$$

We note that the system is marginally stable. A MATLAB/Simulink implementation of the MPC controller, nonlinear storage system models, and sample data for one 24 hour day of solar power generation and household load used in [29] is available online[6]. At the chosen sampling rate there are 86400 data points.

B. Transmission Encoding Performance

We extend this system by considering that the two storage systems have a one-way wireless connection to the digital controller. At the battery and hydrogen system, a local Kalman filter computes a state estimate to filter measurement and process noise. This local state estimate is then the transmitted state measurement of the storage system levels. This state estimate using the microgrid dynamics (20) can then be written in the form (1), where A is the identity matrix of size 2×2 and the process noise $w_k \sim \mathcal{N}(0, Q)$ encodes the Kalman innovation and the control actions. Through testing on the simulation the covariance of the process noise was found to be approximately $Q \approx I_2 \times 10^{-5}$ where I_2 is the identity matrix of size 2×2.

We perform a Monte Carlo simulation of 1000 trials of the one day of sample generation data from [29] to illustrate the estimation error performance difference between the legitimate estimator and the smart eavesdropper. We consider that the two remote estimators have the same channel qualities of $\mu = \mu_e = 0.6$, and we investigate design variable probabilities in the range $\mu_d = \{0.1, 0.9\}$.

Figure 4 shows the mean of the estimation error covariances $P_{k|k}$ (solid blue) and $P^e_{k|k}$ (dashed red) across the Monte Carlo trials and across the simulation time k, against the design variable probability μ_d. As the proportion of the state

[6] http://institucional.us.es/agerar/simugrid/

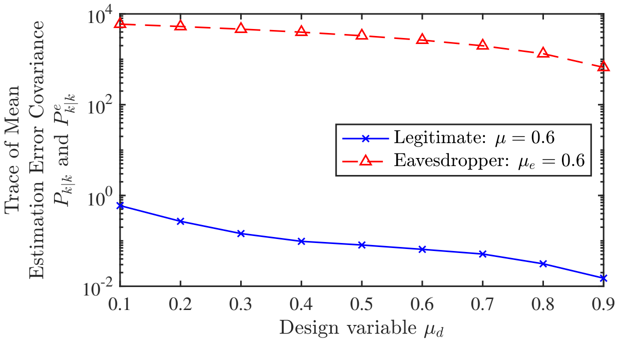

Fig. 4. Monte Carlo Simulation of Microgrid with transmission encoding of remote state estimate. Eavesdropper performance is significantly reduced compared to the legitimate estimator by randomly sending true state and one step innovation.

measurement is sent increases, $\mu_d \to 1$, the estimation error decreases for both the legitimate estimator and the eavesdropper. However, the mean estimation error for the eavesdropper is considerably larger than for the legitimate estimator, greater than 10^3 compared to less than 10^0.

The error in the state measurement does degrade the controller performance. Considering the power flow to the grid connection as a measure of controller performance, as grid flow equates to power sold or purchased, we compare the total power flow over the day using our encoding scheme against no transmission encoding. The difference in grid power flow is below 1.58% for decision probability $\mu_d = 0.1$, highlighting that there is marginal impact on control performance even at the most restrictive encoding scheme.

VIII. Conclusions

This article investigated the problem of remote state estimation in the presence of an eavesdropper, under a challenging network environment. We consider the situation where the transmitter and legitimate estimator receiver do not have a packet receipt acknowledgment channel. This scenario could arise due to hardware limitations or the actions of an adversary jamming the network.

We have developed a state-secrecy code that randomly alternates between sending the state and a random value packet that appears to statistically be the state. The random value packet both damages the eavesdropper's state estimate, while containing encoded state information for the legitimate estimator. Our encoding scheme ensures that the legitimate estimator's expected estimation performance remains bounded. We design our encoding to provide a measure of expected secrecy against an eavesdropper.

An open problem is to ensure state secrecy against intelligent eavesdroppers that learn the encoding scheme.

Appendix

A. Legitimate Estimator Expected Estimation Error Covariance

Proof of Theorem 4.3. The following proof shows the expected estimation error covariance of the state at the legitimate estimator.

Proof: We consider that the legitimate estimator is able to decode the packages that it successfully receives. There are then three outcomes for the legitimate estimator, successful receipt of a state estimate ($\varphi_k = 1$) with probability $p_r = \mathbb{P}(\gamma_k = 1, \nu_k = 0) = \mu\mu_d$, successful receipt of an innovation ($\varphi_k = 2$) with probability $p_i = \mathbb{P}(\gamma_k = 1, \nu_k = 1) = \mu(1-\mu_d)$, and a standard dropout ($\varphi_k = 3$) with probability $p_d = \mathbb{P}(\gamma_k = 0) = (1-\mu)$. The expectation of the estimation error covariance for time $k > 0$ can be written as a sum of the sequence of dropouts from the first transmission

$$E[P_{k|k}] = (p_i + p_d)^k A^k \Sigma_0 (A^\mathsf{T})^k + p_d \sum_{j=0}^{k-1} (p_i + p_d)^j A^j Q (A^\mathsf{T})^j. \tag{21}$$

We show via a proof by induction.

Consider $k = 0$ from definition $E[\bar{P}_{0|0}] = \Sigma_0 B^\mathsf{T} p_d$, as only the state is transmitted at the first time and Σ_0 is the covariance of the initial state x_0. Now consider the first time $k = 1$ from definition $E[P_{1|1}] = \sum_{y=1}^{3} E[P_{1|1} | \varphi_1 = y] P(\varphi_1 = y) = (p_d + p_i) A \Sigma_0 A^\mathsf{T} + p_d Q$. We now show that if (21) holds for time k, that the form (21) also holds for time $k+1$.

$$\begin{aligned} E[P_{k+1|k+1}] &= \sum_{y=1}^{3} E[P_{k+1|k+1} | \varphi_{k+1} = y] P(\varphi_{k+1} = y) \\ &= A E[P_{k|k}] A^\mathsf{T} p_i + E[P_{k+1|k}] p_d 0 p_r \\ &= A E[P_{k|k}] A^\mathsf{T} p_i + \left(A E[\bar{P}_{k|k}] A^\mathsf{T} + Q\right) p_d \\ &= Q p_d + A E[\bar{P}_{k|k}] A^\mathsf{T} (p_i + p_d). \end{aligned}$$

Consider the expression $A E[P_{k|k}] A^\mathsf{T} (p_i + p_d)$ utilizing (21) for $E[P_{k|k}]$, the first term $A\left((p_i + p_d)^k A^k \Sigma_0 (A^\mathsf{T})^k\right) A^\mathsf{T} (p_i + p_d) = (p_i + p_d)^{k+1} A^{k+1} \Sigma_0 (A^\mathsf{T})^{k+1}$, and the second term $A\left(p_d \sum_{j=0}^{k-1} (p_i + p_d)^j A^j Q (A^\mathsf{T})^j\right) A^\mathsf{T} (p_i + p_d) = p_d \sum_{j=1}^{k} (p_i + p_d)^j A^j Q (A^\mathsf{T})^j$. Now $E[P_{k+1|k+1}] = (p_i + p_d)^{k+1} A^{k+1} \Sigma_0 (A^\mathsf{T})^{k+1} + Q p_d + p_d \sum_{j=1}^{k} (p_i + p_d)^j A^j Q (A^\mathsf{T})^j$ which can be written in the form of (21) at time $k+1$. This completes the induction argument.

Let us explore the stabilizing solutions of the two terms of (21) as $k \to \infty$. The first term results from a sequence of a dropouts from the initial transmission. By assumption of μ_d in (9), we note that $\rho(\sqrt{p_i + p_d} A) = \rho(\sqrt{1 - \mu\mu_d} A) < 1$, so as time $k \to \infty$ then $(\sqrt{p_i + p_d} A)^k \to 0$ and the initial estimation error covariance Σ_0 is exponentially forgotten.

The second term encodes the sequences of potential dropouts and innovations occurring from the first dropout after the estimator received a state packet. The sum is comprised of the potential value of the estimation error covariance multiplied by the corresponding probability. Taking as $k \to \infty$, this result can be shown with a countably infinite, irreducible, and aperiodic Markov Chain, see [39]. Consider the sum in (21) from $j = 0$ to $k - 1$ and denote as S_k, then $S_{k-1} = \sum_{j=0}^{k-1} \left(\sqrt{p_i + p_d} A\right)^j Q \left(A^\mathsf{T} \sqrt{p_i + p_d}\right)^j$. By assumption of μ_d in (9), we note that $\rho(\sqrt{p_i + p_d} A) = \rho(\sqrt{1 - \mu\mu_d} A) < 1$, so the sum is a vector geometric series, and can be written in the form of a discrete-time Lyapunov equation sequence [40] where $S_k = \sqrt{p_i + p_d} A \bar{S}_{k-1} A^\mathsf{T} \sqrt{p_i + p_d} + Q$, from $S_0 = Q$.

The stabilizing solution S can be found by taking $k \to \infty$, or setting $S_k = S_{k-1} = S$ and solving for the unique stabilizing solution to $S = \sqrt{p_i + p_d} A S A^\mathsf{T} \sqrt{p_i + p_d} + Q$.

We conclude the proof by stating the expectation of the state using the above results $E[P_{k|k}] = (1-\mu)S$. ■

B. Eavesdropper Expected Estimation Error Covariance

Proof of Theorem 5.2. The following proof shows the expected estimation error covariance of the eavesdropper

Proof: We are going to show via proof by induction that the expected estimation error of the eavesdropper for time $k > 0$ can be written as a sum of the sequence of dropouts and encoded innovations from the first transmission, we repeat the form of $E[P^e_{k|k}]$ from Theorem 5.2

$$E[P^e_{k|k}] = (p^e_d)^k A^{k-1} \Sigma_0 (A^{k-1})^\mathsf{T} + \sum_{\ell=0}^{k-1} (p^e_d)^{\ell+1} A^\ell Q (A^\ell)^\mathsf{T}$$
$$+ p^e_i \sum_{\ell=0}^{k-1} (p^e_d)^\ell 2 \Big(A^k \Sigma_0 (A^k)^\mathsf{T} + \sum_{j=0}^{k-\ell-2} A^{k-1-j} Q (A^{k-1-j})^\mathsf{T} \Big).$$

It is helpful for the proof to rewrite $E[P^e_{k|k}]$ as

$$E[P^e_{k|k}] = (p^e_d)^k A^{k-1} \Sigma_0 (A^{k-1})^\mathsf{T} + \sum_{\ell=0}^{k-1} (p^e_d)^{\ell+1} A^\ell Q (A^\ell)^\mathsf{T}$$
$$+ p^e_i \sum_{\ell=0}^{k-1} (p^e_d)^\ell A^\ell f_{k-\ell} (A^\ell)^\mathsf{T}. \tag{22}$$

where the expected estimation error covariance on use of an innovation $(\gamma^e_k, \nu_k, b_k) = (1,1,1)$ at time $i > 1$ from the result in Lemma 5.1 as $f_i = 2\left(A^i \Sigma_0 (A^i)^\mathsf{T} + \sum_{j=0}^{i-2} A^{i-1-j} Q (A^{i-1-j})^\mathsf{T} \right)$.

We show (22) via proof by induction.

An eavesdropper has three possible outcomes: drop or discards a packet ($\varphi_k = 1$) with probability $p^e_d = \mathbb{P}(\gamma^e_k = 0) + \mathbb{P}(\gamma^e_k = 1, \nu_k = 0, b_k = 0) + \mathbb{P}(\gamma^e_k = 1, \nu_k = 1, b_k = 0)$, receive and use a state packet ($\varphi_k = 2$) with probability $p^e_r = \mathbb{P}(\gamma^e_k = 1, \nu_k = 0, b_k = 1)$, and receive and use an encoded innovation packet ($\varphi_k = 3$) with probability $p^e_i = \mathbb{P}(\gamma^e_k = 1, \nu_k = 1, b_k = 1)$.

Consider $k = 0$ from the definition $E[P^e_{0|0}] = \Sigma_0 p^e_d + 0(p^e_r + p^e_i)$ as only the state is transmitted at the first instance, $z_0 = x_0$. Consider the first time $k = 1$ from the definition $E[P^e_{1|1}] = (p^e_d)^2 A \Sigma_0 A^\mathsf{T} + p^e_i f_1 + 0 p^e_r$.

We now show that if (22) holds for time k, then the form (22) also holds for time $k+1$. From the result in Lemma 5.1 and applying $E[P^e_{k|k}]$ from (22)

$$E[P^e_{k+1|k+1}] = \sum_{y=1}^{3} E[P^e_{k+1|k+1} | \varphi_{k+1} = y] \mathbb{P}(\varphi_{k+1} = y)$$
$$= p^e_d (A E[P^e_{k|k}] A^\mathsf{T} + Q) + p^e_i f_{k+1} + p^e_r 0$$
$$= p^e_d A \left((p^e_d)^k A^{k-1} \Sigma_0 (A^{k-1})^\mathsf{T} + \sum_{\ell=0}^{k-1} (p^e_d)^{\ell+1} A^\ell Q (A^\ell)^\mathsf{T} \right.$$
$$\left. + p^e_i \sum_{\ell=0}^{k-1} (p^e_d)^\ell A^\ell f_{k-\ell} (A^\ell)^\mathsf{T} \right) A^\mathsf{T} + p^e_d Q + p^e_i f_{k+1}$$
$$= (p^e_d)^{k+1} A^k \Sigma_0 (A^k)^\mathsf{T} + \sum_{\ell=0}^{k} (p^e_d)^{\ell+1} A^\ell Q (A^\ell)^\mathsf{T}$$
$$+ p^e_i \sum_{\ell=0}^{k} (p^e_d)^\ell A^\ell f_{k+1-\ell} (A^\ell)^\mathsf{T} A^\mathsf{T}$$

which is the form (22) at $k+1$. This completes the proof. ■

C. Naive and Suspicious Eavesdropper Expected Estimation Error Covariance

Proof of Corollary 5.3 and Corollary 5.4. The following proof shows the expected estimation error covariance of the naive and suspicious eavesdroppers.

Proof: The naive eavesdropper utilizes any transmission that it successfully receives. The probabilities of the three outcomes for the naive eavesdropper are: standard dropout $p^e_d = 1 - \mu_e$, successful receipt of the state $p^e_r = \mu_e \mu_d$, and successful receipt of an innovation $p^e_i = \mu_e(1-\mu_d)$.

The suspicious eavesdropper utilizes a successfully received transmission with random chance based on the type of transmission it receives. The probabilities of the three outcomes for the suspicious eavesdropper are: standard dropout or discard $p^e_d = 1 - \mu_e \mu_d \mu_b - \mu_e \bar{\mu}_b + \mu_e \mu_d \bar{\mu}_b$, successful receipt of the state $p^e_r = \mu_e \mu_d \mu_b$, and successful receipt of an innovation $p^e_i = \mu_e (1-\mu_d) \bar{\mu}_b$.

Applying p^e_d and p^e_i for both the naive and suspicious eavesdroppers to Theorem 5.2, we inspect the resulting terms. Under assumption that $\rho(\sqrt{p^e_d} A) < 1$, then for the first two terms as $k \to \infty$ then $(p^e_d)^k A^{k-1} \Sigma_0 (A^{k-1})^\mathsf{T} \to 0$, and $\sum_{\ell=0}^{k-1} (p^e_d)^{\ell+1} A^\ell Q (A^\ell)^\mathsf{T} \to S^{e,n}$, where 0 is a zero matrix of appropriate size and $S^{e,n}$ is the converged stabilizing solution to the Lyapunov equation. Otherwise $S^{e,n}$ is undefined, and both terms diverge.

Let us inspect the two parts of the last term of Theorem 5.2 as $k \to \infty$ trace $A^k \Sigma_0 (A^k)^\mathsf{T} \to \infty$, if $\rho(A) > 1$, or trace $A^k \Sigma_0 (A^k)^\mathsf{T} > \min_i \lambda_i (A \Sigma_0 A^\mathsf{T})$, if $\rho(A) = 1$, where $\min_i \lambda_i (A \Sigma_0 A^\mathsf{T})$ is the minimum eigenvalue of $A \Sigma_0 A^\mathsf{T}$, and the second part of the last term trace $\sum_{\ell=0}^{k-2} A^{k-1-\ell} Q (A^{k-1-\ell})^\mathsf{T} \to \infty$. By assumption that the pair $(A, \sqrt{Q})$ is controllable, there are no eigenvectors of A in the nullspace of $\sqrt{Q}$. In the case that $\rho(A) = 1$, the eigenvector of A associated with the eigenvalue on the unit circle extracts a combination of the eigenvalues of $\sqrt{Q}$, and remains non-zero as $k \to \infty$. Thus we conclude that as $k \to \infty$ then we have an infinite sum of non-zero eigenvalues of Q.

The expectation of the eavesdropper's estimation error diverge to infinity, or trace $E[P^e_{k|k}] \to \infty$, such that both the naive and suspicious eavesdroppers have an unbounded estimation error satisfying condition (ii) of Definition 2. This completes the proof. ■

D. Monotonicity of Lyapunov Equation

Proof of Lemma 5.7. The following proof shows a monotonicity result on the scaling coefficient on the Lyapunov equation.

Proof: Consider a $\beta^\star$ and β where $0 < \beta, \beta^\star < 1$ where $\rho(\sqrt{1-\beta} A) < 1$ and $\rho(\sqrt{1-\beta^\star} A) < 1$ and introduce two Lyapunov equations (14)–(15) as stabilizing recursions [40] with $W_0^\star = W_0 = Q$, which converge to the unique-stabilizing solutions W and $W^\star$, respectively. Let us introduce $\alpha = \sqrt{1-\beta^\star}/\sqrt{1-\beta}$ and $\tilde{A} = \sqrt{1-\beta}A$, and note that $\rho(\tilde{A}) < 1$ and $\rho(\alpha\tilde{A}) < 1$.

Consider the case that $\beta^\star < \beta$ then $\alpha > 1$. The two Lyapunov equations can be written as $W_{k+1} = \tilde{A}W_k\tilde{A}^\mathsf{T} + Q$ and $W_{k+1}^\star = \alpha\tilde{A}W_k^\star\tilde{A}^\mathsf{T}\alpha + Q$. Let us introduce the difference $V_k = W_k^\star - W_k$, which can written as a function of the previous difference

$$V_k = (\alpha^{2k} - 1)\tilde{A}^k Q(\tilde{A}^\mathsf{T})^k + V_{k-1}, \tag{23}$$

from $V_0 = 0$. We show (23) via proof by induction. Let us first evaluate at $k = 0$ and $k = 1$

$$\begin{aligned} V_0 &= W_0^\star - W_0 = Q - Q = 0, \quad \text{and} \\ V_1 &= W_1^\star - W_1 = \alpha\tilde{A}W_0^\star\tilde{A}^\mathsf{T}\alpha + Q - \tilde{A}W_0\tilde{A}^\mathsf{T} - Q \\ &= (\alpha^2 - 1)\tilde{A}Q\tilde{A}^\mathsf{T} + V_0. \end{aligned}$$

Let us assume the form (23) and show the form at $k+1$ from the definition of $W_k^\star$ and W_k,

$$\begin{aligned} V_{k+1} &= W_{k+1}^\star - W_{k+1} \\ &= \sum_{j=0}^{k+1}(\alpha\tilde{A})^j Q(\tilde{A}^\mathsf{T}\alpha)^j - \sum_{\ell=0}^{k+1}\tilde{A}^\ell Q(\tilde{A}^\mathsf{T})^\ell \\ &= (\alpha^{2(k+1)} - 1)\tilde{A}^{k+1}Q(\tilde{A}^\mathsf{T})^{k+1} \\ &\quad + \sum_{j=0}^{k}(\alpha\tilde{A})^j Q(\tilde{A}^\mathsf{T}\alpha)^j - \sum_{\ell=0}^{k}\tilde{A}^\ell Q(\tilde{A}^\mathsf{T})^\ell \\ &= (\alpha^{2(k+1)} - 1)\tilde{A}^{k+1}Q(\tilde{A}^\mathsf{T})^{k+1} + V_k, \end{aligned}$$

which produces the form (23) at iteration $k+1$.

We now explore the trace of V_k.

$$\begin{aligned} \text{trace } V_k &= \text{trace } \left((\alpha^{2k} - 1)\tilde{A}^k Q(\tilde{A}^\mathsf{T})^k + V_{k-1}\right) \\ &= (\alpha^{2k} - 1)\text{trace}\left(\tilde{A}^k Q(\tilde{A}^\mathsf{T})^k\right) + \text{trace } V_{k-1}. \end{aligned}$$

We observe that trace $(\tilde{A}Q\tilde{A}^\mathsf{T}) > 0$ as the pair $(A, \sqrt{Q})$ is controllable. By definition $\alpha > 1$ so it follows that $\alpha^{2j} - 1 > 0$ for all $j > 0$. Thus the first term is strictly positive $(\alpha^{2k} - 1)\text{trace}\left(\tilde{A}^k Q(\tilde{A}^\mathsf{T})^k\right) > 0$. Consider the trace of V_1 using the same properties as above trace $V_1 = (\alpha^2 - 1)$ trace $(\tilde{A}Q\tilde{A}^\mathsf{T}) > 0$. At $k = 2$, then trace V_{k-1} = trace $V_1 > 0$, and trace $V_2 > 0$. Following a proof by induction argument, we conclude that trace $V_k > 0$ for $k > 0$. This implies that at the difference in stabilized Lyapunov equation solutions trace $(W^\star - W) > 0$, and that trace $W^\star >$ trace W. This concludes the proof. ∎

References

[1] H. Sandberg, S. Amin, and K. H. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Contr. Syst.*, vol. 35, no. 1, pp. 20–23, 2015.

[2] J. Tidy, "Predatory Sparrow: Who are the hackers who say they started a fire in Iran?" Online, July 2022, British Broadcasting Corporation (BBC). [Online]. Available: https://www.bbc.com/news/technology-62072480

[3] R. M. Ferrari and A. M. H. Teixeira, Eds., *Safety, Security and Privacy for Cyber-Physical Systems*, ser. Lecture Notes in Control and Information Sciences. Springer International Publishing, 2021.

[4] H. Ishii and Q. Zhu, Eds., *Security and Resilience of Control Systems*. Springer International Publishing, 2022.

[5] H. Sandberg, V. Gupta, and K. H. Johansson, "Secure networked control systems," *Annu. Rev. Contr., Robot., & Auton. Syst.*, vol. 5, no. 1, pp. 445–464, 2022.

[6] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State estimation with secrecy against eavesdroppers," in *IFAC World Congress*, Toulouse, France, July 2017.

[7] A. S. Leong, D. E. Quevedo, D. Dolz, and S. Dey, "Transmission scheduling for remote state estimation over packet dropping links in the presence of an eavesdropper," *IEEE Trans. Autom. Contr.*, vol. 64, no. 9, pp. 3732–3739, 2019.

[8] H. Liu, Y. Li, K. H. Johansson, J. Mårtensson, and L. Xie, "Rollout approach to sensor scheduling for remote state estimation under integrity attack," *Automatica*, vol. 144, p. 110473, 2022.

[9] M. Lucke, J. Lu, and D. E. Quevedo, "Coding for secrecy in remote state estimation with an adversary," *IEEE Trans. Autom. Contr.*, vol. 67, no. 9, pp. 4955–4962, 2022.

[10] A. Tsiamis, K. Gatsis, and G. J. Pappas, "State-secrecy codes for stable systems," in *Am. Contr. Conf.*, Milwaukee, WI, June 2018.

[11] ——, "State-secrecy codes for networked linear systems," *IEEE Trans. Autom. Contr.*, vol. 65, no. 5, pp. 2001–2015, 2020.

[12] L. Huang, K. Ding, A. S. Leong, D. E. Quevedo, and L. Shi, "Encryption scheduling for remote state estimation under an operation constraint," *Automatica*, vol. 127, p. 109537, 2021.

[13] Y. Li, H. Yu, B. Su, and Y. Shang, "Hybrid micropower source for wireless sensor network," *IEEE Sensors J.*, vol. 8, no. 6, pp. 678–681, 2008.

[14] T. M. Hoang, H. Q. Ngo, T. Q. Duong, H. D. Tuan, and A. Marshall, "Cell-free massive MIMO networks: Optimal power control against active eavesdropping," *IEEE Trans. Commun.*, vol. 66, no. 10, pp. 4724–4737, 2018.

[15] K. Ding, X. Ren, A. S. Leong, D. E. Quevedo, and L. Shi, "Remote state estimation in the presence of an active eavesdropper," *IEEE Trans. Autom. Contr.*, vol. 66, no. 1, pp. 229–244, 2021.

[16] F. Klingler and F. Dressler, "Poster abstract: Jamming WLAN data frames and acknowledgments using commodity hardware," in *IEEE Conf. Comput. Commun. Workshops*, Paris, France, April 2019.

[17] J. M. Kennedy, J. J. Ford, and D. E. Quevedo, "Bayesian quickest change detection of an intruder in acknowledgments for private remote state estimation," in *Aust. & New Zealand Contr. Conf.*, Gold Coast, Australia, November 2022.

[18] P. Cheng, Z. Yang, J. Chen, Y. Qi, and L. Shi, "An event-based stealthy attack on remote state estimation," *IEEE Trans. Autom. Contr.*, vol. 65, no. 10, pp. 4348–4355, 2020.

[19] H. Zhang, Y. Qi, J. Wu, L. Fu, and L. He, "DoS attack energy management against remote state estimation," *IEEE Trans. Contr. Netw. Syst.*, vol. 5, no. 1, pp. 383–394, 2018.

[20] A. Naha, A. Teixeira, A. Ahlén, and S. Dey, "Quickest physical watermarking-based detection of measurement replacement attacks in networked control systems," *Eur. J. Contr.*, vol. 71, p. 100804, 2023.

[21] A. Naha, A. M. H. Teixeira, A. Ahlén, and S. Dey, "Quickest detection of deception attacks on cyber–physical systems with a parsimonious watermarking policy," *Automatica*, vol. 155, p. 111147, 2023.

[22] P. Griffioen, S. Weerakkody, and B. Sinopoli, "A moving target defense for securing cyber-physical systems," *IEEE Trans. Autom. Contr.*, vol. 66, no. 5, pp. 2016–2031, 2021.

[23] A. Naha, A. Teixeira, A. Ahlen, and S. Dey, "Sequential detection of replay attacks with a parsimonious watermarking policy," in *Am. Contr. Conf.*, Atlanta, GA, June 2022.

[24] A. Naha, A. M. H. Teixeira, A. Ahlen, and S. Dey, "Sequential detection of replay attacks," *IEEE Trans. Autom. Contr.*, 2022, Early Access.

[25] J. Yang, W.-A. Zhang, and F. Guo, "Adaptive distributed Kalman-like filter for power system with cyber attacks," *Automatica*, vol. 137, p. 110091, 2022.

[26] A. Gusrialdi and Z. Qu, "Resilient hierarchical networked control systems: Secure controls for critical locations and at edge," in *Security and Resilience of Control Systems*. Springer International Publishing, 2022, pp. 95–119.

[27] G. Park, C. Lee, H. Shim, Y. Eun, and K. H. Johansson, "Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zero-dynamics attack," *IEEE Trans. Autom. Contr.*, vol. 64, no. 12, pp. 4907–4919, 2019.

[28] F. Abdi, C.-Y. Chen, M. Hasan, S. Liu, S. Mohan, and M. Caccamo, "Preserving physical safety under cyber attacks," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6285–6300, 2019.

[29] C. Bordons, F. Garcia-Torres, and M. A. Ridao, *Model Predictive Control of Microgrids*. Springer International Publishing, 2020.

[30] C. Wu, W. Yao, W. Pan, G. Sun, J. Liu, and L. Wu, "Secure control for cyber-physical systems under malicious attacks," *IEEE Trans. Contr. Netw. Syst.*, vol. 9, no. 2, pp. 775–788, 2022.

[31] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 138–162, 2007.

[32] W. Yang, D. Li, H. Zhang, Y. Tang, and W. X. Zheng, "An encoding mechanism for secrecy of remote state estimation," *Automatica*, vol. 120, p. 109116, 2020.

[33] C. Murguia, F. Farokhi, and I. Shames, "Secure and private implementation of dynamic controllers using semihomomorphic encryption," *IEEE Trans. Autom. Contr.*, vol. 65, no. 9, pp. 3950–3957, 2020.

[34] C. Gao, Z. Wang, X. He, and H. Dong, "Fault-tolerant consensus control for multiagent systems: An encryption-decryption scheme," *IEEE Trans. Autom. Contr.*, vol. 67, no. 5, pp. 2560–2567, 2022.

[35] J. Zhou, W. Yang, W. Ding, W. X. Zheng, and Y. Xu, "Watermarking-based protection strategy against stealthy integrity attack on distributed state estimation," *IEEE Trans. Autom. Contr.*, 2022, Early Access.

[36] D. Tse and P. Viswanath, *Fundamentals of wireless communication*. Cambridge, UK: Cambridge University Press, 2005.

[37] K. D. Wong, *Fundamentals of Wireless Communication Engineering Technologies*. John Wiley & Sons, Inc., 2011.

[38] Y. Xu and J. P. Hespanha, "Estimation under uncontrolled and controlled communications in networked control systems," in *IEEE Conf. Decis. & Contr.*, Sevilla, Spain, Dec 2005, pp. 842–847.

[39] J. M. Kennedy, J. J. Ford, D. E. Quevedo, and F. Dressler, "Innovation-based remote state estimation secrecy with no acknowledgments," 2022, arxiv:2212.08234.

[40] B. D. O. Anderson and J. B. Moore, *Optimal Filtering*, T. Kailath, Ed. Englewood Cliffs, N.J., USA: Prentice-Hall Inc., 1979.

[41] M. Crimson, J. M. Kennedy, and D. E. Quevedo, "Remote state estimation with privacy against eavesdroppers," in *IFAC World Congress*, Yokohama, Japan, 2023.

[42] A. J. Gallo, M. S. Turan, F. Boem, T. Parisini, and G. Ferrari-Trecate, "A distributed cyber-attack detection scheme with application to DC microgrids," *IEEE Trans. Autom. Contr.*, vol. 65, no. 9, pp. 3800–3815, 2020.

[43] N. Liu, X. Yu, C. Wang, C. Li, L. Ma, and J. Lei, "Energy-sharing model with price-based demand response for microgrids of peer-to-peer prosumers," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3569–3583, 2017.

[44] C. Zhang, Y. Xu, Z. Y. Dong, and J. Ma, "Robust operation of microgrids via two-stage coordinated energy storage and direct load control," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 2858–2868, 2017.

[45] D. E. Olivares, A. Mehrizi-Sani, A. H. Etemadi, C. A. Canizares, R. Iravani, M. Kazerani, A. H. Hajimiragha, O. Gomis-Bellmunt, M. Saeedifard, R. Palma-Behnke, G. A. Jimenez-Estevez, and N. D. Hatziargyriou, "Trends in microgrid control," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1905–1919, 2014.

[46] J. M. Guerrero, M. Chandorkar, T.-L. Lee, and P. C. Loh, "Advanced control architectures for intelligent microgrids—part i: Decentralized and hierarchical control," *IEEE Trans. Ind. Electron.*, vol. 60, no. 4, pp. 1254–1262, 2013.

[47] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 11–20, 2010.

Justin M. Kennedy was a Research Associate with the School of Electrical Engineering and Robotics, Queensland University of Technology (QUT), Australia. He received his B. Eng (Electrical)/B. Maths, and PhD degrees from QUT, in 2016 and 2022, respectively. Dr Kennedy is a Member of IEEE, IEEE Control Systems Society, and Society for Industrial and Applied Mathematics. His research interest was in the application of mathematical and control system tools to solve network engineering problems.

Jason J. Ford received the B.Sc., B.E., and Ph.D. degrees in 1995 and 1998 from the Australian National University, Australia. He joined the Australian Defence Science and Technology Organisation as a Research Scientist in 1998. He was a Research Fellow at the University of New South Wales, Canberra, in 2004. In 2005, he joined the Queensland University of Technology where he is a full Professor. His current research interests include signal processing and control for aerospace.

Daniel E. Quevedo received Ingeniero Civil Electrónico and M.Sc. degrees from Universidad Técnica Federico Santa María, Valparaíso, Chile, in 2000, and in 2005 the Ph.D. degree from the University of Newcastle, Australia. He is Professor of Cyberphysical Systems at the School of Electrical Engineering and Robotics, Queensland University of Technology (QUT), in Australia. Before joining QUT, he established and led the Chair in Automatic Control at Paderborn University, Germany. In 2003 he received the IEEE Conference on Decision and Control Best Student Paper Award and was also a finalist in 2002. He is co-recipient of the 2018 IEEE Transactions on Automatic Control George S. Axelby Outstanding Paper Award.

Prof. Quevedo currently serves as Associate Editor for *IEEE Control Systems* and in the Editorial Board of the *International Journal of Robust and Nonlinear Control*. From 2015–2018 he was Chair of the IEEE Control Systems Society *Technical Committee on Networks & Communication Systems*. His research interests are in networked control systems, control of power converters and cyberphysical systems security.

Falko Dressler is full professor and Chair for Telecommunication Networks at the School of Electrical Engineering and Computer Science, TU Berlin. He received his M.Sc. and Ph.D. degrees from the Dept. of Computer Science, University of Erlangen in 1998 and 2003, respectively. Dr. Dressler has been associate editor-in-chief for IEEE Trans. on Mobile Computing and Elsevier Computer Communications as well as an editor for journals such as IEEE/ACM Trans. on Networking, IEEE Trans. on Network Science and Engineering, Elsevier Ad Hoc Networks, and Elsevier Nano Communication Networks. He has been chairing conferences such as IEEE INFOCOM, ACM MobiSys, ACM MobiHoc, IEEE VNC, IEEE GLOBECOM. He authored the textbooks Self-Organization in Sensor and Actor Networks published by Wiley & Sons and Vehicular Networking published by Cambridge University Press. He has been an IEEE Distinguished Lecturer as well as an ACM Distinguished Speaker. Dr. Dressler is an IEEE Fellow as well as an ACM Distinguished Member. He is a member of the German National Academy of Science and Engineering (acatech). He has been serving on the IEEE COMSOC Conference Council and the ACM SIGMOBILE Executive Committee. His research objectives include adaptive wireless networking (sub-6GHz, mmWave, visible light, molecular communication) and wireless-based sensing with applications in ad hoc and sensor networks, the Internet of Things, and Cyber-Physical Systems.